G DATA
SECURITY SOFTWARE

Table des matières

1. Introduction

Dans un contexte actuel de gestion globale de réseaux et de risques sécuritaires importants, la protection antivirus ne concerne plus uniquement les spécialistes IT. Il faut prendre en compte ces risques dans un contexte de stratégie de gestions de risques à l'échelle entrepreneuriale. Les périodes d'immobilisation des réseaux causées par des malware frappent les entreprises là où elles sont le plus vulnérables. Le résultat : des réseaux au point mort, perte de données, et perte d'un vecteur de communication important. Les virus peuvent causer des dommages irréversibles aux entreprises.

G DATA propose des protections antivirus hauts de gamme pour l'ensemble de votre réseau. Depuis plusieurs années, les solutions de sécurité G DATA sont récompensées dans de nombreux tests. Les logiciels G DATA pour les professionnels sont basés sur une configuration et une administration centrales ; mais aussi sur le fait d'automatiser au maximum les tâches. Tous les clients, qu'ils soient des postes de travail, des ordinateurs portables, des serveurs sont contrôlés de façon centralisée. Les procédures s'exécutent discrètement en arrière-plan. Les mises à jour Internet sont automatiques, ce qui permet de réagir très rapidement aux attaques virales. Le contrôle central via G DATA ManagementServer facilite l'installation, la configuration, les mises à jour, le contrôle à distance et l'automatisation pour le réseau entier. Cela réduit ainsi les tâches d'administration système.

Nous vous souhaitons une bonne prise en main et une bonne installation de nos solutions G DATA professionnelles.

Votre équipe G DATA

1.1. Documentation d'aide

L'aide du programme, que vous pouvez ouvrir à tout moment à l'aide de la touche F1, contient des informations détaillées concernant l'utilisation du logiciel. Vous avez également la possibilité de télécharger une documentation au format PDF à partir de la **zone d'assistance** du site Web de G DATA.

1.2. Ligne d'assistance G DATA

L'assistance technique pour les licences réseau G DATA est à disposition de tous les clients professionnels enregistrés.

> Adresse électronique : **business-support@gdata.fr**
>
> Vous trouverez une réponse à de nombreuses questions et un certain nombre de procédures détaillées dans la zone d'assistance du site Web de G DATA. Consultez notre site :
>
> **b2b.gdatasoftware.com**

Avant de contacter l'assistance G DATA, vérifiez les équipements de votre réseau/ordinateur. Les informations suivantes sont particulièrement importantes :

- Le numéro de version des applications G DATA Administrator (dans le menu Aide).
- Le numéro d'enregistrement ou le nom d'utilisateur pour les mises à jour Internet. Le numéro d'enregistrement est indiqué dans le courrier de confirmation de commande. En cas de doute, veuillez contacter votre partenaire G DATA.
- Le numéro de version exacte de votre système d'exploitation (client/serveur).
- Les composants matériels et logiciels supplémentaires installés (client/serveur).

- Le contenu exact des éventuels messages d'erreur (dont les codes d'erreur, le cas échéant).

Ces informations favoriseront l'efficacité et la rapidité du traitement de votre demande. Dans la mesure du possible, assurez-vous d'être à proximité d'un PC sur lequel l'application G DATA Administrator est installée.

1.3. G DATA Security Labs

En cas de phénomène inconnu, faites-nous parvenir le fichier à l'aide de la fonction Quarantaine du logiciel G DATA. Pour ce faire, dans la rubrique **Événements de sécurité**, cliquez avec le bouton droit de la souris sur le potentiel virus trouvé et sélectionnez l'option **Quarantaine : envoyer au service G DATA Security Labs**. Évidemment, nous traitons toutes les données envoyées avec confidentialité et discrétion.

1.4. Solutions G DATA Business

La présente documentation détaille les fonctionnalités de tous les modules des versions professionnelles G DATA. Si la version installée sur votre système ne dispose pas de toutes les fonctionnalités, vous pouvez obtenir des informations concernant la mise à niveau de votre logiciel via notre site Internet **b2b.gdatasoftware.com**.

2. Installation

Lancez Windows, puis insérez le support d'installation G DATA. La fenêtre d'installation s'affiche automatiquement et vous permet de sélectionner quel composant G DATA vous souhaitez installer. Si vous avez une version téléchargée, vous devez extraire tous les fichiers et lancer Setup.exe. Pour aider à l'installation sur d'autres appareils, les fichiers extraits peuvent être gravés sur un DVD ou copiés sur une clé USB. Afin d'éviter des interférences (fichiers nécessaires à G DATA Setup utilisés par un autre logiciel), fermez tous les autres programmes avant de commencer l'installation de votre solution G DATA. Les composants suivants peuvent être installés :

- **G DATA ManagementServer** : G DATA ManagementServer doit être installé en premier. G DATA ManagementServer est le pilier de l'architecture G DATA : il gère les clients, procède automatiquement aux mises à jour du logiciel et des signatures antivirus à partir du serveur de mise à jour G DATA et assure la protection antivirus du réseau. Lors de l'installation de l'application G DATA ManagementServer, le logiciel G DATA Administrator est automatiquement installé.
- **G DATA Administrator** : G DATA Administrator est l'interface graphique de G DATA ManagementServer. Il permet de paramétrer et gérer les clients du réseau. G DATA Administrator est protégé par mot de passe. Il peut être installé et lancé sur tout ordinateur Windows pouvant se connecter à G DATA ManagementServer.
- **G DATA Security Client** : cette composante assure la protection antivirus des clients et exécute les tâches que G DATA ManagementServer lui attribue, en arrière-plan. L'installation du logiciel client s'effectue généralement de manière centralisée, via l'application G DATA Administrator.
- **G DATA BootMedium Wizard** : l'application G DATA BootMedium Wizard vous permet de créer un CD d'amorçage pour la vérification de base de votre ordinateur. Cette vérification a lieu avant le lancement du système d'exploitation installé. Les signatures antivirus actuelles sont utilisées.
- **G DATA WebAdministrator** : G DATA WebAdministrator est la version Web de G DATA Administrator. Il en reprend toutes les fonctionnalités et les rend disponibles via un navigateur Internet.
- **G DATA MobileAdministrator** : G DATA MobileAdministrator est optimisé pour les navigateurs Internet sur les appareils mobiles. Il peut être lancé à l'aide d'un navigateur Web mobile et vous propose les principales fonctions d'administration de l'application G DATA Administrator.
- **G DATA MailSecurity pour Exchange** : G DATA MailSecurity pour Exchange sécurise de façon centralisée tout le trafic des emails basés sur Exchange. Il est un module optionnel.
- **G DATA MailSecurity MailGateway** : G DATA MailSecurity MailGateway sécurise de façon centrale le courrier électronique (SMTP, POP3). MailSecurity MailGateway est un module optionnel et peut être installé à partir de son propre fichier d'installation.

2.1. Premier démarrage

En cas de menace de virus élevée, commencez par procéder à une **analyse d'amorçage** sur l'ordinateur concerné.

1. Installez l'application **G DATA ManagementServer** sur l'ordinateur qui servira de serveur antivirus. Pour garantir une protection optimale, l'ordinateur doit toujours être disponible (allumé) et disposer d'un accès à Internet pour le chargement automatique des signatures antivirus. L'installation de G DATA ManagementServer ne nécessite pas un système

d'exploitation serveur (voir **Configuration système requise**). **G DATA Administrator** est automatiquement installée sur le serveur lors de l'installation de l'application G DATA ManagementServer.

2. Effectuez l'enregistrement en ligne. Sans enregistrement en ligne, aucune mise à jour du logiciel ou des signatures antivirus n'est possible.
3. Lors du premier démarrage de G DATA Administrator, l'**Assistant d'installation** s'ouvre automatiquement. Il permet de sélectionner les postes sur lesquels **G DATA Security Client** va être déployé à distance. Tous les paramètres configurés avec l'assistant d'installation peuvent être modifiés ultérieurement.

   En cas de problèmes lors du déploiement via l'assistant d'installation, la détection et le déploiement du client peuvent s'effectuer à l'aide d'**Active Directory**. Il est aussi possible de procéder localement à l'installation sur chaque client, à l'aide du **support d'installation G DATA** ou d'un **paquet d'installation**. Pour que le serveur soit lui-même protégé contre une attaque virale, il est recommandé d'installer le logiciel client pour le serveur.
4. Une fois l'installation et le paramétrage du logiciel client effectués sur les ordinateurs connectés, la protection antivirus, ainsi que les mises à jour Internet peuvent être gérées de manière centralisée. G DATA Administrator propose notamment des possibilités de paramétrage pour la protection en temps réel via l'Outil de surveillance G DATA. Il permet également de définir des tâches d'analyse qui effectuent régulièrement une analyse antivirus du réseau.

   S'il est nécessaire de résoudre sur place un problème de paramétrage d'un client, l'application G DATA Administrator peut être installée sur n'importe quel client du réseau. Il n'est ainsi plus nécessaire de procéder à tous les paramétrages de manière locale sur le serveur. S'il est nécessaire de résoudre un problème critique en dehors du réseau depuis l'extérieur de votre entreprise, l'application G DATA WebAdministrator peut être utilisé via le navigateur Web de n'importe quel bureau. L'application G DATA MobileAdministrator permet de procéder à l'administration lorsque vous êtes en déplacement, via le navigateur Web d'un appareil mobile.

2.1.1. Configuration système requise

Les exigences minimales suivantes sont nécessaires à la gamme de solutions G DATA :

G DATA ManagementServer

- Système d'exploitation : Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003
- Mémoire vive : 1 Go

G DATA Administrator/G DATA WebAdministrator/G DATA MailSecurity Administrator

- Système d'exploitation : Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32 bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003

G DATA MobileAdministrator

- Système d'exploitation : Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 ou Windows Server 2008 R2

G DATA Security Client

- Système d'exploitation : Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista SP1, Windows XP SP3 (32 bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012,

Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003

- Mémoire vive : 1 Go

G DATA Security Client pour Linux

- Système d'exploitation : tous systèmes Linux confondus : 32 et 64 bits. Debian 7, 8 et 9, OpenSUSE Leap 42.1 (64 bits) et Leap 42.2 (64 bits), Suse Linux Enterprise Server 11 SP4 et 12 (64 bits), Red Hat Enterprise Linux 5.11, 6.6 et 7.0 (64 bits), Ubuntu 14.04.1 LTS et 16.04, CentOS 5.11, 6.6 et 7.0 (64 bits), Fedora 24 et 25

G DATA Security Client pour Mac

- Système d'exploitation : Mac OS X 10.7 ou supérieure

G DATA Mobile Device Management pour Android

- Système d'exploitation : Android version 4.0 ou supérieure

G DATA Mobile Device Management pour iOS

- Système d'exploitation : iOS version 7.0 ou supérieure

G DATA MailSecurity MailGateway

- Système d'exploitation : Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32 bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003
- Mémoire vive : 1 Go

G DATA MailSecurity pour Exchange (plug-in Exchange 64 bits)

- Serveur de messagerie : Microsoft Exchange Server 2016, Microsoft Exchange Server 2013, Microsoft Exchange Server 2010 ou Microsoft Exchange Server 2007 SP1

Les solutions G DATA utilisent le protocole TCP/IP pour la communication entre ordinateurs clients et serveurs.

Lors de l'utilisation de la solution G DATA ManagementServer/G DATA MailSecurity MailGateway avec une base de données SQL locale ou d'autres applications exigeantes sur le même ordinateur, la configuration système suivante est recommandée :

- Mémoire de travail : 4 Go
- Processeur : multicœur

2.1.2. Configuration du pare-feu

Si vous utilisez un pare-feu matériel ou logiciel, une configuration est peut-être nécessaire. Effectuez les modifications nécessaires juste après avoir installé votre solution G DATA.

2.1.2.1. Configuration des ports

Les solutions G DATA utilisent différents ports TCP pour communiquer en toute sécurité au sein de votre réseau. Vous devez donc vérifier que ces ports ne sont pas bloqués par votre pare-feu :

ManagementServer principal/secondaire

- Port 80 (TCP)

- Port 443 (TCP)
- Port 7161 (TCP)
- Port 7182 (TCP)
- Port 7183 (TCP)

Serveur de sous-réseau

- Port 80
- Port 443
- Port 7161 (TCP)

Clients

- Port 7169 (TCP)

Serveur MailSecurity MailGateway

- Port 7182 (TCP)

Plug-in Exchange MailSecurity

- Port 7171 (TCP)
- Port 7185...7195 (TCP)

Les numéros des ports ont été sélectionnés de manière à éviter les conflits avec des applications standards existantes. Cependant, vous pouvez modifier les ports de l'application G DATA ManagementServer en cas de conflits. Pour ce faire, ouvrez l'application Services (**Démarrer**, **Exécuter**, *services.msc*) avec des droits d'administrateur et arrêtez le service G DATA ManagementServer. Ouvrez maintenant, dans le fichier d'installation de G DATA ManagementServer (généralement situé sous C:\Program Files\G DATA\G DATA AntiVirus ManagementServer), le fichier Config.xml dans un éditeur de texte (Bloc-notes, par exemple). Modifiez ensuite les numéros de ports des entrées suivantes (si nécessaire) :

- **AdminPort** : saisissez ici le numéro de port souhaité. La valeur par défaut est 0 (le port reste alors préréglé sur 7182).
- **ClientHttpsPort** : la valeur par défaut est 0 (le port reste alors préréglé sur 443). La valeur ClientHttpsPort ne doit pas être modifiée, les clients Android n'acceptent en effet aucun autre port.
- **ClientHttpPort** : saisissez ici le numéro de port souhaité. La valeur par défaut est 0 (le port reste alors préréglé sur 80).

Si vous modifiez la valeur ClientHttpPort ou ClientHttpsPort, vous devez réinitialiser la configuration de sécurité HTTP du port correspondant. Pour ce faire, ouvrez une fenêtre de ligne de commande avec des droits d'administrateur et exécutez la commande *C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert*.

Redémarrez l'application G DATA ManagementServer une fois les ports modifiés. Attention ! Si vous avez modifié la valeur AdminPort, vous devez saisir le port modifié à chaque connexion à l'application G DATA Administrator. La saisie doit respecter le format suivant : *nom du serveur:port*.

2.1.2.2. Configuration des URLs

Pour le module **PatchManager**, G DATA ManagementServer doit pouvoir télécharger des fichiers de configuration et des correctifs. Si vous utilisez un pare-feu, le trafic entre G DATA ManagementServer et les URLs suivantes doit être autorisé :

- *gdata.cdn.heatsoftware.com*

En fonction des correctifs à déployer, la communication devra être autorisée entre G DATA ManagementServer et les URLs suivantes :

- 7-Zip: *http://downloads.sourceforge.net*
- Adobe: *ardownload.adobe.com*, *armdl.adobe.com*, *download.adobe.com*, *swupdl.adobe.com*, *www.adobe.com*
- Microsoft: *go.microsoft.com*, *download.windowsupdate.com*, *www.download.windowsupdate.com*, *download.skype.com*, *download.microsoft.com*
- Mozilla: *http://ftp.mozilla.org*
- UltraVNC: *http://support1.uvnc.com*
- VideoLAN: *http://download.videolan.org*

2.1.3. Support d'amorçage G DATA

Le support d'amorçage G DATA vous aide à combattre les virus qui se sont nichés sur un ordinateur avant l'installation du logiciel antivirus et qui cherchent éventuellement à empêcher l'installation de G DATA. Il est exécuté avant le démarrage du système.

1. **Avec le support d'installation** : insérez le support d'installation G DATA. Dans la fenêtre de démarrage qui s'ouvre, cliquez sur **Quitter** et éteignez l'ordinateur.
   Avec le support d'amorçage G DATA créé : **G DATA BootMedium Wizard** doit être préalablement installé. L'installation doit être effectuée sur un système sur lequel l'application G DATA Security Client avec des signatures à jour est installée. Après installation, suivez les consignes de G DATA BootMedium Wizard pour créer un support d'amorçage.
2. Redémarrez l'ordinateur. Le menu de démarrage du support d'amorçage G DATA s'affiche.
3. À l'aide de touches fléchées, sélectionnez votre langue, puis l'option **CD d'amorçage G DATA**. Un système d'exploitation Linux démarre et une version spéciale de l'application G DATA AntiVirus s'affiche.

   En cas de problèmes d'affichage de l'interface du programme, redémarrez l'ordinateur et sélectionnez l'option **CD d'amorçage G DATA - alternative**.
4. Si vous avez créé un support d'amorçage G DATA, les signatures antivirus disposent de la version chargée par G DATA Security Client au moment de la création du support. Le cas échéant, le programme propose de mettre à jour les signatures antivirus. Cliquez sur **Oui** et lancez la mise à jour. Veillez à saisir votre numéro d'enregistrement ou vos données d'accès pour permettre l'exécution de la mise à jour.
5. L'interface du programme s'affiche maintenant. Cliquez sur **Ordinateur** pour analyser votre ordinateur. Selon le type d'ordinateur et la taille du disque dur, cette opération peut durer plus d'une heure.
6. Si G DATA détecte des virus, supprimez-les à l'aide de l'option proposée par le programme. Après la suppression des virus, les fichiers originaux seront de nouveau accessibles.

7. Une fois l'analyse antivirus terminée, cliquez sur le bouton Fermer (dans la partie supérieure droite de l'interface du programme Linux), puis sélectionnez **Terminer** > **Redémarrer**.
8. Retirez le support d'amorçage G DATA du lecteur ou du port USB.
9. Redémarrez votre ordinateur. Le système d'exploitation standard de l'ordinateur est alors lancé. Le logiciel G DATA peut maintenant être installé sur un système sain.

2.1.3.1. G DATA BootMedium Wizard

Pour créer un support d'amorçage G DATA, vous devez installer G DATA BootMedium Wizard. L'installation doit s'effectuer sur un système sur lequel G DATA Security Client avec des signatures antivirus à jour est installé. Insérez le support d'installation G DATA et sélectionnez **G DATA Boot Medium Wizard**.

Une fois l'installation terminée, vous pouvez créer un support d'amorçage en vous aidant de l'assistant, disponible sous **Démarrer** > **Tous les programmes** ou **Programmes** > **G DATA** > **G DATA BootMedium** et cliquez sur **G DATA BootMedium Wizard**. Vous pouvez ensuite créer le CD d'amorçage, en le gravant sur un CD, le copiant sur une clé USB ou en l'enregistrant en tant qu'image ISO. L'image ISO peut, le cas échéant, être gravée avec un logiciel externe ou être distribuée aux clients du réseau.

2.1.3.2. Régler l'option d'amorçage au niveau du BIOS

Si le système ne démarre pas à partir du CD/DVD-ROM ou du port USB, vous devez activer cette option. Cela s'effectue au niveau du BIOS, un système qui démarre automatiquement avant le système d'exploitation. Procédez comme suit pour effectuer des modifications à ce niveau :

1. Éteignez l'ordinateur.
2. Redémarrez votre ordinateur. Habituellement, vous accédez à la configuration BIOS en appuyant pendant le démarrage (= amorçage) de l'ordinateur sur la touche **Suppr** (parfois aussi sur la touche **F2** ou **F10**). Pour plus d'informations, reportez-vous à la documentation du fabricant de l'ordinateur.
3. Les modalités de modification de la configuration au niveau du BIOS sont définies dans la documentation du fabricant de la carte mère. En conséquence, la succession logique de l'amorçage doit être USB, CD/DVD-ROM, C : c'est-à-dire que le port USB devient votre premier dispositif d'amorçage, le lecteur de CD/DVD-ROM devient le second et la partition du disque dur avec son système d'exploitation Windows, le troisième.
4. Enregistrez les modifications et redémarrez votre ordinateur. Votre ordinateur est maintenant prêt pour une analyse avant le démarrage du système.

2.2. Installation de G DATA ManagementServer

Insérez le support d'installation G DATA et sélectionnez ensuite le composant **G DATA ManagementServer**. Fermez les autres applications pour éviter de rencontrer des conflits lors de l'installation. Sélectionnez la langue d'installation puis cliquez sur **Installer** pour lancer l'assistant d'installation. Lisez le contrat de licence relatif à l'utilisation du logiciel. Sélectionnez **J'accepte les termes de ce contrat de licence** et cliquez sur **Suivant** si vous acceptez les termes du contrat.

Vous pouvez sélectionner le type de serveur une fois le dossier d'installation indiqué. Vous disposez des possibilités suivantes :

- **Serveur principal** : lors d'une première installation, l'application G DATA ManagementServer

doit être installée en tant que serveur principal (MMS principal). Le serveur principal représente l'instance de configuration et de gestion centrale de l'architecture de protection antivirus réseau. L'application G DATA ManagementServer fournit aux ordinateurs à protéger les dernières mises à jour des signatures antivirus et du programme. En outre, les paramètres du client sont tous gérés de manière centralisée depuis l'application G DATA ManagementServer.

- **Serveur secondaire** : si une base de données SQL autonome est utilisée, un deuxième serveur (MMS secondaire) accédant à la même base de données que le serveur principal peut être exploité. Si le serveur principal est inaccessible durant une heure ou plus, les clients se connectent automatiquement au serveur secondaire et y téléchargent les mises à jour des signatures antivirus. Les clients repassent automatiquement sur le serveur principal lorsque ce dernier est de nouveau disponible. Les deux serveurs chargent les mises à jour des signatures indépendamment l'un de l'autre et établissent ainsi une protection contre les pannes.
- **Serveur de sous-réseau** : pour les grands réseaux (par exemple, maison mère avec succursales raccordées), il peut être judicieux d'utiliser l'application G DATA ManagementServer en tant que serveur de sous-réseau. Les serveurs de sous-réseau permettent de délester le réseau entre les clients et le serveur MMS principal. Ils peuvent être utilisés dans des réseaux où ils gèrent les clients qui leur ont été rattachés. Les serveurs de sous-réseau restent fonctionnels, même lorsque le ManagementServer Principal ou Secondaire n'est pas accessible. Ceux-ci ne chargent cependant pas eux-mêmes les mises à jour des signatures antivirus. Entrez le nom du serveur principal dans **Nom du serveur principal**.

  Comme alternative à l'installation d'un sous-réseau, vous pouvez utiliser la **Déploiement de la mise à jour de poste à poste**. Si cette option est activée, la charge du réseau entre le serveur et le client est fortement réduite lors de la distribution des mises à jour. Sur certains réseaux, l'installation d'un serveur de sous-réseau est alors superflue.

Après avoir choisi le type de serveur, choisissez la base de données que G DATA ManagementServer devra utiliser :

- **Installer Microsoft SQL Server 2014 Express** : Choisissez l'installation du serveur SQL Express si vous installez G DATA ManagementServer sur un réseau comportant moins de 1000 clients. Microsoft SQL Server 2014 Express n'est pas compatible avec Windows Vista ou Windows Serveur 2008/2003. Pour ces systèmes d'exploitation, vous devez installer Microsoft SQL Server 2008 R2 Express avant d'installer ManagementServer ou utiliser une instance de base de données déjà existante et choisir l'option **Utiliser une instance de base de données déjà existante** lors de l'installation. Veuillez-vous référer au Reference Guide pour plus d'information.
- **Utiliser une instance de base de données déjà existante** : pour des réseaux plus importants, il est recommandé d'utiliser une instance Microsoft SQL Server existante. Si vous réinstallez ManagementServer sur un serveur qui a déjà SQL Server Express et une base de données G DATA ManagementServer, choisissez l'option d'utilisation d'une instance existante. Après l'installation, configurez la connexion au SQL Server Express.

L'installation démarre automatiquement après confirmation de l'éventuelle installation de Microsoft SQL Server 2014 et/ou des autres prérequis. La solution G DATA doit être activée pour permettre de télécharger les mises à jour.

- **Saisir un numéro d'enregistrement** : lors de la première installation du logiciel G DATA, sélectionnez cette option et saisissez le numéro d'enregistrement. Le numéro se trouve sur le courrier de confirmation de commande. En cas de doutes, contactez votre revendeur ou le distributeur responsable. La saisie du numéro d'enregistrement permet d'activer la solution. Les

codes d'accès créés sont affichés une fois l'enregistrement correctement effectué. **Vous devez impérativement noter ces codes d'accès !** Il n'est plus possible de saisir de nouveau la clé de licence une fois l'enregistrement correctement effectué.

Si vous rencontrez des problèmes lors de la saisie du numéro d'enregistrement, vérifiez que le numéro d'enregistrement a été correctement saisi. Selon la typographie utilisée, un grand l (Inès) peut être confondu avec le chiffre 1 ou la lettre l (Louis). Cela est également le cas pour : B et 8, G et 6, Z et 2.

- **Saisir les données d'accès** : une fois le logiciel G DATA installé, vous recevez des codes d'accès (nom d'utilisateur et mot de passe). Saisissez ici les codes d'accès pour installer de nouveau le logiciel G DATA.
- **Activer ultérieurement** : si vous souhaitez d'abord vous faire une idée du logiciel ou si les codes d'accès ne sont pas disponibles pour le moment, vous pouvez également procéder à l'installation sans saisir les données. Cette forme du programme ne charge pas les mises à jour Internet, aucune protection n'est donc assurée contre les logiciels malveillants. Le logiciel G DATA ne peut protéger votre ordinateur de manière efficace que s'il dispose de mises à jour. L'utilisation du logiciel sans activation ne vous offre donc pas une protection suffisante. Vous pouvez saisir votre numéro d'enregistrement ou vos codes d'accès à tout moment. Pour ce faire, consultez également la section **Remarques concernant l'activation ultérieure du logiciel G DATA**.

  Attention : si le logiciel est installé sans être activé, seuls les composants G DATA Antivirus Business sont disponibles, même si vous avez fait l'acquisition de l'application G DATA Client Security Business ou G DATA Endpoint Protection Business ou d'un autre module. Les composants supplémentaires ne sont activés et disponibles qu'une fois le logiciel enregistré.

Si vous choisissez une SQL instance existante, vous devrez la configurer une fois l'installation terminée. Dans le Reference Guide, vous trouverez plus d'informations sur la configuration de la base de données.

Après installation du logiciel G DATA ManagementServer, celui-ci est prêt à l'emploi. Il peut être nécessaire de redémarrer le serveur. G DATA ManagementServer est automatiquement lancé à chaque (re)démarrage du système.

Pour gérer l'application G DATA ManagementServer, vous pouvez sélectionner, sous **Démarrer** > **Tous les programmes** ou **Programmes** > **G DATA Administrator**, l'entrée **G DATA Administrator** et démarrer ainsi l'interface utilisateur de G DATA ManagementServer.

2.3. Installation de G DATA Administrator

Lors de l'installation de G DATA ManagementServer, G DATA Administrator est automatiquement installée sur le même ordinateur. L'installation de G DATA Administrator peut avoir lieu sur tout ordinateur du réseau. De cette manière, G DATA ManagementServer peut également être gérée de manière distante.

Pour installer G DATA Administrator sur un ordinateur client, insérez le support d'installation G DATA et sélectionnez ensuite le composant **G DATA Administrator**.

Veuillez fermer toutes les autres applications du système d'exploitation Windows en cours pour éviter de rencontrer des problèmes lors de l'installation. Suivez les étapes d'installation de l'assistant. Après installation, l'entrée **G DATA Administrator** est disponible sous **Démarrer** > **Tous les programmes** ou **Programmes** > **G DATA** > **G DATA Administrator**.

2.4. Installation de G DATA WebAdministrator

Insérez le support d'installation G DATA et sélectionnez ensuite le composant **G DATA WebAdministrator** d'un clic.

L'installation de l'application G DATA WebAdministrator est très simple. Une fois les conditions du contrat de licence acceptées, sélectionnez le dossier dans lequel l'application WebAdministrator doit être installée. Nous vous recommandons de l'installer dans le répertoire HTTP du serveur Web (\inetpub\wwwroot, par exemple).

Lors de l'installation, il est possible qu'il soit nécessaire d'installer des logiciels supplémentaires, en fonction de la configuration système requise :

- **Microsoft Internet Information Services (IIS)** : l'application WebAdministrator étant basée sur le Web, le serveur sur lequel elle est installée doit également pouvoir être utilisé en tant que serveur Web. L'application WebAdministrator prend en charge Microsoft Internet Information Services (IIS). Vérifiez que les services IIS sont exécutés sur votre serveur avant d'installer l'application WebAdministrator. Veuillez-vous référer au Reference Guide pour plus d'informations.
- **Compatibilité avec la gestion IIS 6** : avant d'installer l'application G DATA WebAdministrator, vous devez impérativement activer la fonction Windows Compatibilité avec la gestion IIS 6. Si cette fonction n'est pas disponible, l'installation de l'application G DATA WebAdministrator sera interrompue. Cette option est disponible sous **Démarrer** > **Panneau de configuration** > **Programmes** > **Programmes et fonctionnalités** > **Activer ou désactiver des fonctionnalités Windows** (sous Windows Vista). Vous pouvez activer ou désactiver l'option sous **Services Internet (IIS)** > **Outils d'administration Web** > **Compatibilité avec la gestion IIS 6**. En outre, les services World Wide Web doivent être activés (si ce n'est pas déjà le cas). Pour ce faire, cochez la case Services Internet (IIS) > Services World Wide Web. Sur les systèmes d'exploitation serveur, les options correspondantes se trouvent dans le gestionnaire de serveurs, sous **Rôles**.
- **Microsoft .NET Framework** : l'application WebAdministrator est basée sur le programme .NET Framework de Microsoft. Si le programme Microsoft .NET Framework n'est pas installé sur le serveur, l'assistant d'installation de l'application WebAdministrator vous demande de procéder à l'installation. Un redémarrage sera nécessaire après installation.
- **Microsoft Silverlight** : l'application G DATA WebAdministrator nécessite Microsoft Silverlight. Si ce programme n'est pas installé, vous en êtes informé au premier démarrage de l'application G DATA WebAdministrator.

Une fois l'installation terminée, une icône **G DATA WebAdministrator** s'affiche sur le bureau de votre ordinateur. Vous recevez également un lien qui vous permet d'accéder à WebAdministrator via votre navigateur.

L'utilisation de l'application WebAdministrator via Internet sans une connexion sécurisée présente un risque. Nous vous conseillons d'utiliser un **certificat de serveur SSL pour les services IIS**.

2.5. Installation de G DATA MobileAdministrator

Insérez le support d'installation G DATA et sélectionnez ensuite le composant **G DATA MobileAdministrator** d'un clic.

L'installation de l'application G DATA MobileAdministrator est comparable à celle de l'application

WebAdministrator. Une fois les conditions du contrat de licence acceptées, sélectionnez le dossier dans lequel l'application MobileAdministrator doit être installée. Nous vous recommandons de l'installer dans le répertoire HTTP du serveur Web (\inetpub\wwwroot, par exemple).

Lors de l'installation, il est possible qu'il soit nécessaire d'installer des logiciels supplémentaires, en fonction de la configuration système requise :

- **Microsoft Internet Information Services (IIS)** : l'application MobileAdministrator étant basée sur le Web, le serveur sur lequel elle est installée doit également pouvoir être utilisé en tant que serveur Web. L'application MobileAdministrator prend en charge Microsoft Internet Information Services (IIS). Vérifiez que les services IIS sont exécutés sur votre serveur avant d'installer l'application MobileAdministrator.
- **Microsoft .NET Framework** : l'application MobileAdministrator est basée sur le programme .NET Framework de Microsoft. Si le programme Microsoft .NET Framework n'est pas installé sur le serveur, l'assistant d'installation de l'application MobileAdministrator vous demande de procéder à l'installation. Un redémarrage sera nécessaire après installation.

Une fois l'installation terminée, le programme d'installation met à votre disposition un lien vous permettant d'accéder à l'application MobileAdministrator. Ce lien vous permet d'accéder à l'application depuis votre smartphone et de l'utiliser, via un navigateur mobile.

L'utilisation de l'application MobileAdministrator via Internet sans une connexion sécurisée présente un risque. Nous vous conseillons d'utiliser un **certificat de serveur SSL pour les services IIS**.

2.6. Installation de G DATA Security Client

G DATA Security Client protège et gère les clients Windows et doit être installé sur tous les ordinateurs Windows du réseau. Selon le scénario de déploiement, l'installation du logiciel client peut avoir lieu via une **installation à distance** (à l'aide de l'application G DATA Administrator) ou via une **installation locale** (à l'aide du support d'installation G DATA ou d'un paquet d'installation pour le client). Il est également recommandé d'installer G DATA Security Client sur le serveur.

> Si vous installez l'application G DATA Security Client sur un serveur, vous devez vous assurer de l'absence de conflits avec les procédures de travail existantes. Vous devez par exemple définir des exceptions d'analyse et de surveillance pour certains dossiers et fichiers sur les serveurs de bases de données ainsi que de messagerie électronique. Pour plus d'informations, reportez-vous au Guide de référence.

2.6.1. Installation à distance

Le moyen le plus pratique d'installer le logiciel client sur les postes est de procéder à l'installation à distance à l'aide de G DATA Administrator. L'**Assistant d'installation du serveur** vous permet d'installer automatiquement G DATA Security Client sur tous les ordinateurs connectés au réseau.

En plus de la **configuration des ports**, les conditions suivantes sont requises pour procéder à l'installation à distance :

- Il est nécessaire d'avoir un compte qui a les droits d'administration sur le client. Il n'est pas obligatoire d'avoir un mot de passe pour ce compte, par contre si le compte n'a pas de mot de passe, la machine cible doit être configurée pour autoriser les comptes sans mot de passe à se connecter via le réseau. Pour plus d'informations, reportez-vous au Guide de référence. Pour installer un serveur de sous-réseau, un mot de passe est obligatoire : un champ vide pour le mot de passe n'est pas autorisé.

- Sur le client, Service Contrôle Manager doit être accessible à distance en utilisant le compte d'utilisateur spécifié.
- Le compte choisi doit avoir des droits d'écriture sur au moins un partage réseau du client, tel que C$, Admin$ ou un dossier partagé personnalisé.
- L'accès peut être activé en ouvrant le **Centre Réseau et Partages** > **Modifier les paramètres de partages avancés** > **Activer le partage de fichiers et d'imprimantes** (Windows Vista et suivant). Pour Windows XP, activez le **Partage de fichiers et d'imprimantes** dans la partie **Exceptions** du pare-feu Windows.
- Lors que le client n'est pas dans un domaine, d'autres paramètres doivent être configurés :
  - **Partage de fichier simple** (Windows XP) ou **Utiliser l'Assistant Partage** (Windows Vista/ Serveur Windows 2008 ou plus récent) doit être désactivé. Ces options sont activées par défaut dans toutes les installations Windows et peuvent être désactivées comme suit : ouvrez le dossier de votre choix dans l'Explorateur Windows, cliquez sur **Outils** > **Options des dossiers** > **Affichage** et désactivez les options respectives.
  - Lorsque le client utilise Windows Vista ou un système plus récent : ouvrez l'éditeur de registre du client et aller jusqu'à la clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\System, Ajoutez un DWORD que vous nommez *LocalAccountTokenFilterPolicy* et auquel vous donnez la valeur 1.

L'**Assistant d'installation du serveur**, qui est automatiquement activé au premier lancement de l'application G DATA Administrator, vous offre une vue d'ensemble de tous les ordinateurs connectés au réseau. Vous pouvez également ajouter et activer d'autres ordinateurs manuellement en saisissant leur nom. Vous pouvez ensuite installer G DATA Security Client sur ces ordinateurs en cliquant avec le bouton droit de la souris et en sélectionnant **Installer G DATA Security Client** dans le menu contextuel qui s'affiche. Une fenêtre de saisie, dans laquelle vous devez indiquer votre **Nom d'utilisateur**, votre **Mot de passe** et le **Domaine** disposant de droits d'accès aux clients, s'affiche. Une fois la langue d'affichage sélectionnée, la fenêtre **Vue d'ensemble des installations** s'ouvre automatiquement pour vous permettre de suivre le statut de l'installation à distance. Dans la plupart des cas, l'ordinateur client doit être redémarré afin de finaliser l'installation : la procédure d'installation ajoute un rapport dans le module **Événements de sécurité** si un redémarrage est requis.

> Si vous utilisez l'option **Lier à une « OU » Active Directory**, vous pouvez installer automatiquement le logiciel client sur les nouveaux ordinateurs qui se connectent au réseau.

L'installation à distance peut être effectuée de deux manières. Si le client correspond à la configuration requise, les données d'installation sont directement lues à partir du serveur et les modifications correspondantes sont apportées au registre. Si le serveur a uniquement accès au disque dur de l'ordinateur client et non au registre ou qu'il ne répond pas à la configuration système requise, le programme d'installation est alors copié sur le client et l'installation est automatiquement lancée au démarrage suivant de l'ordinateur.

2.6.2. Installation locale

Si l'**installation à distance** n'est pas possible, vous pouvez également installer G DATA Security Client directement sur les clients. Pour ce faire, utilisez le support d'installation G DATA, installez le logiciel client directement sur le poste ou créez un paquet d'installation qui peut procéder à l'installation en arrière-plan (parfait pour la distribution du logiciel via des scripts de connexion).

2.6.2.1. Support d'installation G DATA

Pour installer localement le client sur un ordinateur, insérez le support d'installation G DATA et sélectionnez le composant **G DATA Security Client**.

Au cours de l'installation, saisissez le nom du serveur ou l'adresse IP du serveur sur lequel G DATA ManagementServer est installée. La saisie du nom du serveur est nécessaire pour que le client puisse entrer en contact avec le serveur via le réseau. Il est également possible d'entrer un nom de groupe. Une fois connecté au ManagementServer, le client sera ajouté au groupe correspondant. Voir **Paquet d'installation** pour plus d'informations sur les règles pour entrer des noms de groupe.

Pour protéger le ManagementServer contre les accès frauduleux, les clients ayant été installé via le fichier setup doivent être autorisés via G DATA Administrator pour être pleinement intégré. Allez sous l'onglet **Clients** le sous onglet **Vue d'ensemble** puis un clic droit et enfin autoriser.

2.6.2.2. Paquet d'installation

Le paquet est un fichier exécutable (GDClientPck.exe) qui permet l'installation de G DATA Security Client. Le paquet d'installation permet, par exemple, de distribuer le client à tous les ordinateurs d'un domaine par le biais d'un script de connexion ou de l'installer directement, de manière locale. Le paquet comprend toujours la dernière version client présente sur le serveur.

Pour créer un paquet d'installation, lancez G DATA Administrator. Dans le menu **Organisation**, sélectionnez l'option **Créer le paquet d'installation pour les clients Windows**. Le système vous demande de renseigner les informations suivantes :

- **ManagementServer** : le ManagementServer dans lequel le client doit s'enregistrer.
- **Langue d'installation** : la langue d'installation.
- **Groupe** : le groupe auquel le client doit être attribué après installation.

  Utilisez une barre oblique (slash) " / " pour séparer les noms de groupes dans une hiérarchie. Les caractères spéciaux doivent être marqués dans les groupes de noms : Tout guillemet doit être dupliqué. Si le nom d'un groupe contient un " / ", le nom de groupe doit être inclus dans les guillemets.
- **Limite de validité** : La durée de validité du paquet d'installation. Si le paquet est utilisé après cette limite, le client devra être manuellement autorisé via G DATA Administrator sous l'onglet **Clients** sous onglet **Vue d'ensemble**.

Cliquez sur **OK** et sélectionnez un emplacement. G DATA Administrator crée alors un paquet d'installation en arrière-plan. Vous devez ensuite copier le paquet d'installation sur l'ordinateur cible et vous y connecter avec des droits d'administrateur. G DATA Security Client est alors installé. Si l'installation doit être exécutée sans interaction avec l'utilisateur, lancez le paquet d'installation avec le paramètre /@_QuietInstallation = "true" : *GDClientPck.exe /@_QuietInstallation="true"*.

2.7. Installation de G DATA Security Client pour Linux

Tous comme les clients Windows, les clients Linux sont gérés par G DATA ManagementServer, ce qui rend possible la configuration via G DATA Administrator ainsi que la distribution de mises à jour des signatures antivirus automatiques. L'installation basique du client contient une fonctionnalité pour des analyses virales à la demande. Les modules de sécurité additionnels peuvent optionnellement être installés pour les serveurs Linux.

La méthode d'installation est la même que pour les clients Windows : une **installation à distance** via G DATA Administrator ou une **installation locale** avec le script d'installation.

2.7.1. Installation à distance

La manière la plus simple pour installer G DATA Security Client pour Linux est d'initier une installation à distance grâce à G DATA Administrator. Les prérequis sont les suivants :

- La machine Linux doit avoir un serveur SSH installé et en fonctionnement.
- Le compte d'utilisateur utilisé pour installer le client doit être capable de se connecter au serveur SSH en utilisant un mot de passe.
- La résolution de nom DNS pour le ManagementServer et le client doit être disponible.

L'installation est exécutée comme suit :

1. Dans le module **Clients**, sélectionnez un client Linux, ouvrez le menu **Clients** et sélectionnez la commande **Installer G DATA Security Client pour Linux/Mac**.
2. Sélectionnez le type du client (**Client pour Linux**).
3. Si, besoin choisissez un ou plusieurs **Plugins** (**Samba**, **Squid** ou **Sendmail/Postfix**). Les configurations minimum requises sont décrites dans les chapitres concernés.
4. Indiquez maintenant un **Nom d'utilisateur** et son **Mot de passe**. L'utilisateur doit avoir les permissions root.
5. Cliquez ensuite sur le bouton **OK**. Le processus d'installation s'affiche dans la fenêtre **Vue d'ensemble des installations**.

2.7.2. Installation locale

Si l'**installation à distance** s'avère impossible, vous pouvez installer G DATA Security Client pour Linux localement.

1. Lancez G DATA Administrator, sélectionnez l'onglet **Clients** et choisissez l'option **Créer une script d'installation pour les clients Linux/Mac** depuis le menu **Organisation**.
2. Après avoir choisi un emplacement de stockage, le script sera créé en arrière-plan.
3. Copiez le script d'installation sur le client. Ensuite, ajoutez une permission pour exécuter le script (ligne de commande : *chmod +x install-clients.sh*).
4. Ouvrez une fenêtre Terminal et élevez le niveau de permission de l'utilisateur avec la commande *su*. Puis entrez le mot de passe root. Vous pouvez également procéder en exécutant la commande depuis l'étape 5 en utilisant *sudo*.
5. Naviguez vers le dossier où vous avez copié le fichier, puis exécutez-le : *./install-client.sh -t <produit[,produit]>*. Les paramètres du produit doivent être une ou plusieurs des valeurs suivantes :
   - *ALL* : G DATA Security Client pour Linux et tous les modules additionnels
   - *WS* : G DATA Security Client pour Linux
   - *SMB* : module Samba
   - *AMAVIS* : module Sendmail / Postfix
   - *WEB* : module Squid
6. Pour protéger le ManagementServer contre les accès frauduleux, les clients ayant été installés via une installation locale doivent être autorisés via G DATA Administrator sous l'onglet **Clients**

>**Vue d'ensemble** avant d'être pleinement servis.

2.7.3. Modules supplémentaires

G DATA Security Client pour Linux contient des modules supplémentaires qui apportent de la sécurité à de nombreux composants Linux. Si vous sélectionnez des modules additionnels lors de l'installation locale ou à distance, les modules sont automatiquement installés. Cependant, certains modules ont besoin de paramétrage supplémentaire avant ou après l'installation.

2.7.3.1. Samba

La version du serveur de fichier de G DATA Security Client pour Linux inclus un module de sécurité pour les partages Samba. Après l'installation de G DATA Security Client pour Linux, il est possible de sécuriser Samba en ajoutant la ligne *vfs objects = gdvfs* au fichier de configuration Samba (généralement/ etc/samba/smb.conf). Pour protéger tous les partages, ajoutez-la à la section *[global]*. Si la ligne est dans une autre section, la protection ne s'applique qu'aux partages correspondants. Après avoir enregistré le fichier de configuration, redémarrez le service Samba.

2.7.3.2. Linux Mail Security Gateway

Le module Linux Mail Security Gateway est un **module optionnel**.

Le module Linux Mail Security Gateway (Sendmail/Postfix) a été développé en tant que plugin pour le Framework Amavis. Linux Mail Security Gateway nécessite AlterMIME et Amavis 2.8.0 ou supérieur. Si Amavis n'est pas disponible dans le système, il sera automatiquement installé lors de l'installation du module Linux Mail Security Gateway. Les étapes de configurations suivantes sont nécessaires :

1. Le module Linux Mail Security Gateway nécessite un serveur de messagerie opérationnel Sendmail/Postfix.
2. Veuillez vérifier que le serveur de messagerie transfère les emails à Amavis. Plus d'informations peuvent être trouvées dans la documentation d'Amavis ou dans celle du serveur de messagerie correspondant.
3. Veuillez vérifier que l'analyse anti-spam et antivirale a été activée dans la configuration d'Amavis. Plus d'informations peuvent être trouvées dans la documentation d'Amavis.
4. Modifiez le fichier de configuration /etc/gdata/amavis/mms.cfg et veuillez vérifier que le nom de domaine du (sous) serveur de messagerie a été entré sous *localDomains* (ex. *mail.domain.com*).

Utiliser une installation Amavis existante n'est pas recommandé car cela nécessite un nombre important de changements dans les fichiers de configuration directement après l'installation du module Linux Mail Security Gateway.

Une fois configuré, le module Linux Mail Security Gateway vérifiera automatiquement le trafic email et reportera les virus au G DATA ManagementServer. Ces configurations peuvent être gérées via G DATA Administrator dans le module **Sendmail/Postfix**.

> Attention : En utilisant une version Amavis antérieure à 2.10.0, la totalité des fonctions du module Linux Mail Security Gateway n'est pas disponible, seulement une partie. Veuillez mettre à jour Amavis vers la version 2.10.0 ou plus récente avant de déployer le module Linux Mail Security Gateway pour garantir les pleines fonctionnalités.

2.7.3.3. Linux Web Security Gateway

Le module Linux Web Security Gateway est un **module optionnel**.

Si vous sélectionnez le module Linux Web Security Gateway (Squid), l'installation de G DATA Security Client pour Linux installe et configure automatiquement Squid, lui-même. Si Squid est déjà présent sur le système, la version existante sera désinstallée au préalable.

Après l'installation, le nom d'hôte ou l'adresse IP du serveur Squid doit être configuré comme un serveur proxy sur tous les systèmes pour lesquels le trafic doit être filtré par Squid (port 3128). Pour activer l'analyse du trafic HTTPS, configurez en plus un proxy HTTPS avec le nom d'hôte Squid ou l'adresse IP et port 6789. Les certificats nécessaires sont situés dans le dossier /etc/gdata/ssl sur le serveur Squid et doivent être importés sur tous les clients. Si vous utilisez vos propres certificats SSL, ils doivent être sauvegardés sur le serveur dans le dossier /etc/gdata/ssl.

> Attention : l'installation du serveur Squid utilisera le paquet disponible dans le dépôt de cette distribution. Si la version de Squid est antérieure à la version 3.3.8, alors l'analyse HTTPS ne sera pas disponible.

Une fois activé, le module Linux Web Security Gateway compare le flux avec une liste noire et fait remonter la détection de virus à G DATA ManagementServer. La configuration s'effectue via G DATA Administrator sous le module **Squid**.

2.8. Installation de G DATA Security Client pour Mac

G DATA Security Client for Mac permet la centralisation de l'administration, configuration, de la protection contre les malware ainsi que de la mise à jour automatique grâce à G DATA Administrator.

La méthode d'installation est la même que pour les clients Linux et Windows : une **installation à distance** via G DATA Administrator ou une **installation locale** grâce à un script d'installation.

2.8.1. Installation à distance

La manière la plus simple pour installer G DATA Security Client pour Mac est d'initier une installation à distance grâce à G DATA Administrator. Les **prérequis** et la procédure d'installation sont quasiment identiques à celles pour Linux :

1. Dans le module **Clients**, sélectionnez un client Mac, ouvrez le menu **Clients** et sélectionnez la commande **Installer G DATA Security Client pour Linux/Mac**.
2. Pour **Type du Client**, sélectionnez **Client pour Mac**.
3. Indiquez maintenant un **Nom d'utilisateur** et son **Mot de passe**. Le compte doit avoir les permissions root.
4. Cliquez ensuite sur le bouton **OK**. Le processus d'installation s'affiche dans la fenêtre **Vue d'ensemble des installations**.

2.8.2. Installation locale

Si une **installation à distance** n'est pas possible, vous pouvez installer G DATA Security Client pour Mac localement.

1. Lancez G DATA Administrator, sélectionnez l'onglet **Clients** et choisissez l'option **Créer une script d'installation pour les clients Linux/Mac** depuis le menu **Organisation**.
2. Après avoir choisi un emplacement de stockage, le script sera créé en arrière-plan.

3. Copiez le script d'installation vers le client.
4. Ouvrez la fenêtre du terminal et élevez le statut de l'utilisateur en entrant *su* et le mot de passe root. Ou alors, vous pouvez exécuter la commande depuis l'étape 5 en utilisant *sudo*.
5. Naviguez vers le dossier où vous avez copié le fichier et exécutez-le : *./install-client.sh -t WS*.
6. Afin d'éviter les accès non autorisés au ManagementServer, les clients déployés via une installation locale doivent être autorisés dans le G DATA Administrator sous **Clients** > **Vue d'ensemble** avant d'être pleinement servis.

2.9. Installation de G DATA Exchange Mail Security/G DATA MailSecurity MailGateway

Le type de déploiement de G DATA MailSecurity dépend du serveur de messagerie utilisé dans votre réseau. Pour les réseaux qui utilisent Microsoft Server 2007 SP1/2010/2013/2016, il peut être installé en tant que plugin. Exchange Mail Security s'enregistre lui-même sur un ManagementServer et est administré par G DATA Administrator. La solution autonome MailSecurity MailGateway, peut être utilisée avec tous les serveurs de messagerie. Il peut être configuré grâce à G DATA MailSecurity Administrator qui est installé parallèlement.

2.9.1. Exchange Mail Security

L'assistant d'installation d'Exchange Mail Security ajoute un plugin pour Microsoft Exchange Server 2007 SP1/2010/2013/2016. Il doit être installé sur tous les serveurs Exchange qui ont le rôle serveur de boîtes aux lettres ou le rôle serveur de Transport Hub.

Pour installer G DATA Exchange Mail Security, insérez le medium d'installation, sélectionnez **G DATA MailSecurity pour Exchange** et suivez l'assistant d'installation. Le plugin se connecte à G DATA ManagementServer, qui doit être installé au préalable. Après avoir installé le plugin, identifiez-vous dans le ManagementServer en utilisant G DATA Administrator pour configurer les paramètres de protection dans l'onglet **Paramètres Exchange**.

Afin d'éviter les accès non autorisés au ManagementServer, les clients Exchange déployés via une installation locale doivent être autorisés dans le G DATA Administrator sous **Clients** > **Vue d'ensemble** avant d'être pleinement servis.

2.9.2. MailSecurity MailGateway

MailSecurity peut être installé sur la machine hébergeant le serveur de courrier électronique ou sur une autre machine. À l'installation de MailSecurity, plusieurs configurations sont disponibles. Idéalement MailSecurity doit être installé après le pare-feu (s'il existe). De cette manière, le flux SMTP/POP3 en provenance d'Internet sera envoyé à MailSecurity par le pare-feu.

Pour installer MailSecurity lancez le support d'installation ou le fichier Select.exe contenu dans l'archive téléchargée. Dans la section **Installer en tant que passerelle de messagerie** sélectionnez **G DATA MailSecurity** puis suivez les instructions de l'utilitaire d'installation.

Si vous choisissez d'installer les composants pour l'évaluation statistique, le bouton **Statistiques** est disponible dans l'onglet **État** de G DATA MailSecurity Administrator. Il donne des informations statistiques concernant le serveur de courrier électronique et est paramétrable depuis : **Options** > **Journalisation**.

Quel que soit le type d'installation choisi, plusieurs paramètres (adresse IP, ports) doivent être configurés après l'installation, que ce soit au niveau du serveur de courrier électronique ou de

l'ordinateur hébergeant G DATA MailSecurity. Des exemples de configurations de ports pour différents scénario sont disponibles dans le Reference Guide.

En fonction de la configuration du réseau, MailSecurity peut utiliser plusieurs nœuds pour analyser les emails à la recherche de spam et d'infection par des virus :

- Si vous collectez vos courriers directement depuis un serveur POP3 externe, MailSecurity peut être configuré de manière à analyser les emails avant qu'ils ne soient ouverts. Le paramétrage s'effectue depuis : **Options** > **Entrant (POP3)**.
- Si vous utilisez un serveur SMTP local pour récupérer vos emails, MailSecurity peut analyser les emails avant même qu'ils n'arrivent au serveur de courrier électronique. Le paramétrage s'effectue depuis : **Options** > **Entrant (SMTP)**.
- MailSecurity peut analyser tous les courriers sortants avant l'envoi au destinataire. Le paramétrage s'effectue depuis : **Options** > **Sortant (SMTP)**.

2.10. Installation de G DATA Internet Security pour Android

Pour profiter des possibilités offertes par G DATA Mobile Device Management, vous devez installer une version du programme G DATA Internet Security, spécialement créée pour les professionnels, sur vos appareils Android. Les options d'installation sur les clients Android proposées par G DATA Administrator sont disponibles dans la **rubrique Clients**. Sélectionnez les clients Android et cliquez sur le bouton **Envoyer le lien d'installation aux clients mobiles** pour envoyer un courrier aux périphériques Android concernés.

Après l'envoi du courrier, vous ou vos collaborateurs pourrez ouvrir le courrier sur le périphérique mobile et installer le fichier APK en appuyant sur le lien de téléchargement. Nous attirons votre attention sur le fait que l'option **Sources inconnues (Autoriser l'installation d'applications ne provenant pas de Google Play)** doit être activée pour permettre l'installation du fichier. Cette option est normalement disponible sous **Paramètres** > **Sécurité** > **Gestion de l'appareil** dans le menu des systèmes Android. Après l'ouverture du fichier APK et la confirmation des autorisations demandées, G DATA Internet Security pour Android est installé et peut être lancé à partir du menu d'applications Android.

Pour finaliser l'installation, l'administration à distance doit être activée. L'email contient un lien qui ouvre automatiquement G DATA Internet Security pour Android et qui configure les paramètres requis. Sinon, vous pouvez entrer les données manuellement. Ouvrez **Paramètres** > Menu **Général**, cochez l'entrée **Autoriser l'administration à distance** et saisissez le nom ou l'adresse IP de l'application ManagementServer sous **Adresse du serveur**. Sous **Nom de l'appareil**, vous pouvez attribuer un nom au périphérique Android. Il sera identifié sous ce nom dans G DATA Administrator. Sous **Mot de passe**, saisissez le mot de passe que vous avez défini dans G DATA Administrator (ce mot de passe figure également dans le courrier que vous avez reçu).

Le périphérique est alors ajouté aux autres clients dans la rubrique **Clients** de G DATA Administrator, à partir de laquelle il peut être géré. Si le périphérique n'apparaît pas automatiquement dans cette liste, redémarrez-le pour activer la connexion à G DATA ManagementServer.

3. G DATA ManagementServer

G DATA ManagementServer est la base de l'architecture G DATA : elle gère les clients, procède automatiquement aux mises à jour du logiciel et des signatures antivirus à partir du serveur de mise à jour G DATA et gère la protection antivirus du réseau. G DATA ManagementServer utilise le protocole TCP/IP pour communiquer avec les clients. Pour les clients temporairement hors d'atteinte de G DATA ManagementServer, les tâches sont automatiquement cumulées et synchronisées lors de la communication suivante entre G DATA Security Client et G DATA ManagementServer. G DATA ManagementServer dispose d'un dossier de quarantaine centralisé. Les fichiers suspects peuvent être enregistrés de manière chiffrée, supprimés, désinfectés ou, le cas échéant, transmis au service G DATA SecurityLabs. L'application G DATA ManagementServer est gérée via l'application **G DATA Administrator**.

> Lorsque vous quittez G DATA Administrator, l'application G DATA ManagementServer reste active en arrière-plan et gère les processus définis pour les clients.

4. G DATA Administrator

G DATA Administrator est le logiciel de commande de l'application G DATA ManagementServer, qui permet la gestion de l'ensemble des serveurs et clients G DATA installés sur le réseau. G DATA Administrator est protégé à l'aide d'un mot de passe et peut être installé et lancé sur tous les ordinateurs Windows du réseau.

Lors de la première connexion à G DATA Administrator, l'**assistant d'installation** se lance automatiquement. Il est vivement conseillé de se laisser guider par cet assistant de manière à effectuer les paramétrages minimums nécessaires à un fonctionnement correct de votre solution G DATA.

4.1. Lancement de l'application G DATA Administrator

G DATA ManagementServer se lance en cliquant sur l'entrée **G DATA Administrator** dans le groupe de programmes **Démarrer** > **Tous les programmes** ou **Programmes** > **G DATA** > **G DATA Administrator**.

Dans la fenêtre qui s'ouvre, veuillez indiquer les informations suivantes :

- **Langue** : sélectionnez la langue d'affichage.
- **Serveur** : saisissez le nom de l'ordinateur sur lequel l'application G DATA ManagementServer a été installée. Sur la droite, un indicateur de statut affiche si le ManagementServer est prêt. En cas d'erreur, un fichier journal est affiché en cliquant sur l'indicateur de statut.
- **Authentification** :
  - **Authentification Windows** : Connexion à l'aide de vos identifiants d'accès administrateur Windows.
  - **Authentification intégrée** : Connexion via un système d'authentification intégré à l'application G DATA ManagementServer. Vous pouvez créer des comptes intégrés à l'aide de la fonction **Gestion des utilisateurs**.
- **Nom d'utilisateur** : Saisissez un nom d'administrateur Windows ou un utilisateur de l'authentification intégré.
- **Mot de passe** : Saisissez le mot de passe correspondant à l'utilisateur choisi.

Validez le tout en cliquant sur **OK** pour vous connecter.

Cliquez sur la flèche située à côté du point d'interrogation pour ouvrir les menus contenant des options. Les informations relatives à la version sont affichées sous **À propos de G DATA Administrator**. L'option **Réinitialiser les paramètres** vous permet de réinitialiser les paramètres d'affichage de l'application G DATA Administrator (taille des fenêtres, par exemple).

4.2. Utilisation de G DATA Administrator

L'interface G DATA Administrator est composée des rubriques suivantes :

- La section **Vue d'ensemble** donne des informations de statut général et contient des raccourcis pour accéder à des rubriques telles que les rapports, les journaux et les mises à jour.
- La section **Clients/ManagementServers** affiche tous les clients et ManagementServers pouvant être gérés.
- Une configuration peut être effectuée en utilisant les **modules** accessibles par des onglets

dédiés sur la droite. La disponibilité des modules dépend de la sélection actuelle dans le module **Clients/ManagementServers** et de votre **solution**.

- La barre de menu permet d'accéder à des configurations globales, tout comme à des menus complémentaires qui ne s'affichent que quand les modules spécifiques sont sélectionnés :
  - **Admin** : Accédez l'assistant d'installation du serveur ou quittez G DATA Administrator.
  - **Organisation** (voir **Clients/ManagementServers** > **Clients** > **Organisation**)
  - **Clients** (voir **Clients** > **Vue d'ensemble**)
  - **Tâches** (voir **Tâches**)
  - **Pare-feu** (voir **Pare-feu** > **Vue d'ensemble**)
  - **Évènements de sécurité** (voir **Protocoles** > **Évènements de sécurité**)
  - **Network Monitoring** : Ouvrez **G DATA ActionCenter** pour utiliser le **module optionnel** Network Monitoring.
  - **Affichage** : Affiche/cache l'onglet **Vue d'ensemble**.
  - **?** : affiche le fichier d'aide et les informations de version.

4.2.1. Vue d'ensemble

La section Vue d'ensemble affiche une vue d'ensemble rapide sur les rapports non lus, les fichiers journaux et d'autre informations de statut. En cliquant sur les icônes, vous avez un accès rapide aux modules respectifs avec un paramètre de filtre préconfigurés pour n'afficher que les données demandées. La disponibilité des icônes dépend de votre solution G DATA.

- **Information** : Information générales et rapports d'erreurs.
- **Sécurité** : rapports d'infections.
- **Demandes** : demandes en provenance des modules PolicyManager, PatchManager et du pare-feu ainsi que du contrôle d'application Android.
- **Correctifs** : correctifs à haute priorité n'ayant pas encore été appliqués.
- **Journal Client** : Journal répertoriant des informations telles que les changements de paramétrages, le statut des tâches d'analyse etc.
- **Journal Serveur** : Journal d'informations et rapports d'erreurs pour le ManagementServer.
- **Postfix** : Rapports du module Sendmail/Postfix.
- **Squid** : Rapports du module Squid.
- **Exchange** : rapport de MailSecurity pour Exchange.
- **Clients non autorisés** : Les clients connectés au ManagementServer mais n'ayant pas été encore autorisés par l'administrateur.
- **Serveurs non autorisés** : Les serveurs de sous-réseaux connectés au ManagementServer mais n'ayant pas encore été autorisés par l'administrateur.
- **Clients Exchange non autorisés** : Les clients Exchange connectés au ManagementServer mais n'ayant pas été encore autorisés par l'administrateur.
- **Signatures** : Informations de version des signatures antivirales se trouvant sur le ManagementServer.
- **Programme** : Informations de version du ManagementServer.

4.2.2. Clients/ManagementServers

La section Clients/ManagementServers affiche les clients et serveurs gérés par G DATA Administrator. En sélectionnant l'onglet **Clients** ou **ManagementServers** vous basculez entre l'affichage des clients et l'affichage des ManagementServers (serveur principal, serveur secondaire et serveur de sous-réseau).

Les clients et les ManagementServers sont affichés dans une liste basée sur des nœuds. Comme dans l'Explorateur Windows, les nœuds contenant des nœuds subordonnés apparaissent avec un symbole plus. Lorsque vous cliquez sur ce symbole, la structure s'ouvre et affiche les nœuds subordonnés. Cliquez sur l'icône Moins pour refermer ce sous-groupe.

La barre d'icônes comprend les principales commandes de gestion des clients, dont certaines sont également affichées dans le menu **Organisation**. La disponibilité de ces options dépend des clients/ ManagementServers sélectionnées :

 **Rafraîchir**

 **Développer/réduire tout** : vous pouvez modifier ici l'affichage du répertoire réseau.

 **Afficher les clients non activés**

 **Créer un groupe**

 **Supprimer**

 **Activer le client** : Ajouter un client Windows ou Linux à la rubrique **Clients** grâce à son nom ou son adresse IP.

 **Vue d'ensemble des installations**

 **Envoyer le lien d'installation aux clients mobiles** : Envoie un lien d'installation aux clients Android et iOS.

4.2.2.1. Clients

La rubrique Clients affiche les divers types de clients, listés selon l'arborescence suivante en cinq niveaux :

- **Tous les serveurs de gestion** : Clients Windows, Linux, Mac et Android.
- **Exchange** : Les clients sur lesquels le plug-in MailSecurity pour Exchange est installé.
- **Sendmail/Postfix** : Clients Linux avec le module Sendmail/Postfix installé.
- **Squid** : Clients Linux avec le module Squid installé.
- **iOS Mobile Device Management** : Client iOS.

Avant de pouvoir gérer les clients, il est nécessaire de les ajouter à la rubrique Clients et de les déployer. La procédure dépend du type de client, de la taille du réseau et de la configuration :

- Windows : Utilisez l'**Assistant d'installation du serveur**, la fenêtre de dialogue **Trouver le/les ordinateur(s)**, l'option de la barre d'outil **Activer le client** ou **l'assistance Active Directory** pour ajouter les clients Windows, ensuite **Déployer G DATA Security Client**.
- Linux : Utilisez l'option de la barre d'outils **Activer le client** pour ajouter un client Linux, puis **Déployer G DATA Security Client pour Linux**.
- Mac : Utilisez l'option de la barre d'outils **Activer le client** pour ajouter un client Mac, puis **Déployer G DATA Security Client pour Mac**.
- MailSecurity pour Exchange : **Déployer G DATA MailSecurity pour Exchange**. Le client

Exchange est alors ajouté automatiquement.

- Android : Utilisez **Envoyer le lien d'installation aux clients mobiles** dans la barre d'outils pour envoyer un message électronique au client. Cela initialise le **déploiement de G DATA Internet Security pour Android**. Le client Android est ainsi automatiquement ajouté.
- iOS : Entrez votre identifiant pour G DATA ActionCenter sous **G DATA ActionCenter**. Utilisez **Envoyer le lien d'installation aux clients mobiles** dans la barre d'option pour envoyer un message électronique au client. Après que l'utilisateur ait accepté la configuration Device Management, le client iOS est automatiquement ajouté.

Les types suivants d'icônes sont affichés dans la rubrique Clients :

 Racine

 ManagementServer

 Groupe

 Groupe (Lier avec Active Directory)

 Ordinateur fixe

 Ordinateur fixe (non activé)

 Ordinateur portable

 Client mobile

 Serveur Linux

 Client Linux

 MailSecurity pour client Exchange

 Appareils que l'on ne peut pas sélectionner : des appareils tels que des imprimantes réseaux sont listées dans cette catégorie.

Lorsqu'un client, groupe ou ManagementServer est sélectionné, les modules client correspondants s'affichent en tant qu'onglets dans la rubrique **Module**. Selon le type de nœud sélectionné, différents modules et options sont disponibles. Vous pouvez ainsi exécuter la fonction **Paramètres du client** pour modifier les options des clients PC. Pour les clients Android, vous devez sélectionner l'onglet **Paramètres Android**.

Vous pouvez facilement importer et exporter des paramètres dans la rubrique Clients. Cliquez avec le bouton droit de la souris sur un client, puis sélectionnez **Exporter les réglages** pour enregistrer les paramètres du client et les paramètres PolicyManager dans un fichier .dbdat. Pour importer des paramètres, faites un clic droit sur le groupe ou le client sur lequel appliquer les paramètres. Sélectionnez **Importer les réglages** et choisissez les catégories de paramètres souhaitées ainsi que le fichier .dbdat contenant ces paramètres.

Organisation

Lorsque la rubrique Clients est sélectionnée, le menu **Organisation** s'affiche dans la barre de menu, vous permettant ainsi d'accéder aux paramètres liés à l'organisation du client.

Rafraîchir

La fonction Rafraîchir met à jour la liste de la rubrique Clients/ManagementServers.

Afficher les clients non activés

Cette fonction permet d'afficher les clients qui ne sont pas (encore) activés. Les clients non activés sont représentés par une icône pâle.

Ajouter un groupe

Des clients peuvent être combinés dans des groupes pour appliquer des configurations à plusieurs clients en une seule fois. Des zones de sécurité légèrement différentes sont alors définies, puisque tous les paramètres peuvent être exécutés aussi bien pour des clients isolés que pour des groupes entiers. Une fois cette option sélectionnée et le nom du groupe indiqué, les clients peuvent être affectés à un nouveau groupe en faisant glisser le client souhaité de la liste des clients vers le groupe correspondant avec la souris, par glisser/déposer.

Pour placer un grand nombre de clients dans un groupe, rendez-vous sous l'onglet **Clients** > sous-onglet **Vue d'ensemble**. Sélectionnez les clients qui doivent être dans un même groupe, puis faites un clic droit, choisissez **Déplacer client vers**. Déroulez l'arborescence et enfin sélectionnez le groupe voulu.

Modifier un groupe

Cette option ouvre une boîte de dialogue vous permettant de regrouper des clients ou de supprimer des clients d'un groupe grâce aux boutons **Ajouter** et **Supprimer**. Uniquement disponible lorsqu'un groupe est sélectionné dans la rubrique Clients.

Supprimer

Certains clients peuvent être supprimés de la liste des clients avec la commande Supprimer. L'application G DATA Security Client n'est pas désinstallée lors de la suppression de clients de la liste.

> Pour supprimer un groupe, il faut désactiver les clients du groupe ou les placer dans d'autres groupes. Seuls les groupes vides peuvent être supprimés.

Recherche d'ordinateur(s)

La fenêtre Recherche d'ordinateur(s) peut être utilisée pour ajouter et activer des clients dans la rubrique **Clients**. Cette boîte de dialogue permet également d'identifier et d'activer des clients via leur adresse IP.

La fenêtre Recherche d'ordinateurs permet de contacter tous les ordinateurs d'une plage d'adresses IP donnée. La plage peut être définie à l'aide d'une **Adresse IP de début** et d'une **Adresse IP de fin** (192.168.0.1 et 192.168.0.255, par exemple) ou de l'**Adresse du sous-réseau** (notation CIDR, 192.168.0.0/24, par exemple). Sélectionnez l'option **Rechercher uniquement les ordinateurs accessibles (commande Ping)** si vous souhaitez que seuls les clients disponibles soient répertoriés. Cliquez ensuite sur **Démarrer la recherche** pour lancer la recherche sur le réseau. Les ordinateurs ne sont répertoriés qu'une fois identifiés. Si la recherche dure trop longtemps, vous pouvez l'interrompre en cliquant sur **Annuler la recherche**.

Tous les clients qui répondent à la détection IP sont alors répertoriés (leur adresse IP et le nom de l'ordinateur sont également affichés). Le bouton **Activer** permet d'ajouter des clients à la rubrique **Clients**. Dans les résultats de recherche, il est possible de désactiver les clients activés en cliquant sur **Désactiver**.

Assistant de création de règles

Lors de la première connexion des clients à ManagementServer, ils sont automatiquement affectés au groupe **Nouveaux clients**, s'ils n'ont été affectés à aucun groupe lors de l'activation du client ou la création du paquet d'installation. L'assistant de règles peut être utilisé pour créer des règles qui vont affecter les clients à un groupe en fonction des règles définies.

Le règles sont gérées en utilisant les boutons **Nouveau**, **Modifier**, et **Supprimer** ainsi que les flèches à droite de la liste de règles. Les boutons **Importer** et **Exporter** importe/exporte les règles depuis/

vers un fichier .json.

Dans la section **Paramètres**, se trouvent les paramètres généraux définissant l'exécution des règles :

- **Planification** : La fréquence à laquelle sont exécutées les règles (toutes les heures, tous les jours, toutes les semaines).
- **Heure** : L'heure à laquelle les règles vont être exécutées.
- **Appliquer les paramètres de groupe** : Les clients reçoivent les paramètres du groupe vers lequel ils ont été déplacés.
- **Déplacer uniquement les clients du groupe "Nouveaux Clients"** : Les règles ne s'appliquent qu'aux clients se trouvant dans le groupe **Nouveaux Clients**. Si cette option n'est pas sélectionnée, la règle s'applique à tous les clients. Cela peut engendrer énormément de déplacement de clients. Cette option devrait être sélectionnée constamment.
- **Exécuter maintenant** : Exécuter les règles immédiatement.

Grâce aux différents critères, vous pouvez créer des règles qui déplace automatiquement déplacer les clients d'un groupe à l'autre.

- **Type de règle** : Sélectionnez la caractéristique par laquelle les clients vont être identifiés, **Nom de l'ordinateur**, **Adresse IP**, **Domaine** ou **Passerelle par défaut**.
- **Caractères de substitution des clients** : Saisissez la chaine de caractères à utiliser pour identifier les clients. Vous pouvez utiliser des caractères de remplacement. Exemple saisissez *Sales** pour sélectionnez tous les clients dont le nom commence par Sales (lorsque le **Type de règle** choisi est **Nom de l'ordinateur**) ou encore *192.168.0.[1-100]* pour choisir les clients entre l'adresse IP 192.168.0.1 à 192.168.0.100 (lorsque le **Type de règle** choisi est **Adresse IP**).
- **Type de Client** : Sélectionnez quel type de client seront déplacés (**Tous**, **Poste de travail**, **Serveur**, **Appareil Android** ou **Ordinateur portable**).
- **Groupes** : Sélectionnez dans l'arborescence un ou plusieurs groupes par double clic.

Lorsque plusieurs groupes ont été sélectionnés, les clients sont répartis entre les groupes de manière équitable.

Créer le paquet d'installation pour les clients Windows

Cette fonction permet de créer un paquet d'installation pour l'application G DATA Security Client. Ce paquet d'installation permet de procéder facilement à l'installation de l'application G DATA Security Client localement. Reportez-vous au chapitre **Installation locale** pour plus d'informations.

Créer le script d'installation pour les clients Linux/Mac

Cette fonction peut être utilisée pour créer un script d'installation pour G DATA Security Client pour Linux et G DATA Security Client pour Mac. Veuillez utiliser le script pour installer G DATA Security Client localement. Voir le chapitre **Installation locale (Linux)** et **Installation locale (Mac)** pour plus de détails.

Vue d'ensemble des installations

Vous pouvez utiliser la fenêtre Vue d'ensemble des installations pour bénéficier d'une vue d'ensemble de la progression de l'installation. Cette fenêtre s'ouvre automatiquement lors de l'ajout d'une tâche d'installation à distance, elle peut également être affichée à l'aide du bouton Vue d'ensemble des installations de la rubrique **Clients/ManagementServers**.

La fenêtre Vue d'ensemble des installations affiche toutes les tâches d'installation à distance

terminées et en cours. La colonne **Type** indique le type d'installation (par exemple G DATA Security Client, G DATA Internet Security pour Android, serveur de sous-réseau). La colonne **Statut** est mise à jour une fois l'installation à distance terminée. Pour les clients ayant été ajoutés grâce à la **synchronisation Active Directory**, la colonne **Prochaine installation** affiche le moment où l'installation à distance sera lancée. Grâce à un clic droit sur une entrée, vous avez accès aux options suivantes :

- **Actualiser** : rafraichit la liste.
- **Supprimer l'entrée** : supprime l'entrée sélectionnée de la liste.
- **Afficher le rapport d'installation** : affiche le rapport d'installation de l'entrée sélectionnée.
- **Réessayer** : renouvelle une tentative échouée d'installation.

Envoyer un lien d'installation aux clients mobiles

La fenêtre **Envoyer un lien d'installation aux clients mobiles** permet d'envoyer un message électronique d'installation aux clients mobiles. Selon la sélection dans la rubrique **Clients**, la fenêtre contiendra des options pour les clients **Android** ou **iOS**.

Le client peut **installer G DATA Internet Security pour Android** (déploiement sur les clients Android) en ouvrant le message électronique ou activer Device Management (déploiement sur les clients iOS). Après avoir suivi la procédure, le(s) client(s) mobile(s) seront visibles dans la rubrique **Clients**.

> Afin qu'il puisse envoyer le lien d'installation aux clients mobiles, G DATA ManagementServer doit être capable d'envoyer des courriers électroniques. Assurez-vous d'avoir entré vos identifiants pour un serveur SMTP sous **Paramètres généraux** > **Messagerie électronique** > **Paramètres des courriers électroniques**.

Clients Android

Afin d'envoyer un lien d'installation aux clients Android, les informations suivantes doivent être renseignées :

- **Mot de passe** : si vous n'avez pas encore défini un mot de passe pour les mobiles (rubrique **Paramètres généraux** > **Android**)
- **Destinataire(s)** : saisissez une ou plusieurs adresses e-mail. Les adresses sont séparées soit par un retour à la ligne soit par une virgule.
- **Sujet** : saisissez l'objet de l'e-mail d'installation.
- **Contenu** : saisissez ici, le message de corps de texte de l'email. Les caractères de substitution des liens d'installation doivent impérativement être dans l'e-mail.

Cliquez sur **OK** pour envoyer les informations d'installation.

Clients iOS

Lors du déploiement de Device Management vers des clients iOS, plusieurs paramètres vous permettent de personnaliser l'apparence de la requête Device Management que reçoit l'utilisateur :

- **Nom**: Entrez le nom du Device Management.
- **Description**: Entrez la description du Device Management.
- **Organisation**: Entrez le nom de votre organisation.
- **Contrat de licence de l'utilisateur final**: Entrez un accord de licence de l'utilisateur.

- **Destinataire**: Entrez une ou plusieurs adresse(s) email, séparées par des sauts de ligne ou des virgules.

Cliquez sur **OK** pour envoyer le lien d'installation.

> Avant d'envoyer un lien d'installation vers un client iOS, assurez-vous d'avoir entré vos identifiants dans l'ActionCenter sous l'onglet **ActionCenter**.

Active Directory
L'intégration Active Directory permet d'importer tous les objets ordinateurs des unités d'organisation du domaine. Pour ce faire, un groupe doit être créé dans l'application G DATA Administrator. Lorsque vous cliquez avec le bouton droit de la souris sur le groupe que vous venez de créer, l'option de menu **Lier à une « Ou » Active Directory** s'affiche. Dans la boîte de dialogue qui s'affiche, sélectionnez l'option **Attribuer un groupe dans le répertoire Active Directory** et sélectionnez un serveur LDAP. Le bouton **Sélection** vous propose une sélection de serveurs disponibles. La connexion à un autre domaine est également possible. L'option **Installer automatiquement l'application G DATA Security Client sur les ordinateurs récemment ajoutés** entraîne une **installation à distance** de G DATA Security Client sur tous les ordinateurs ajoutés au domaine Active Directory, dans la mesure où ils correspondent à la **configuration minimale requise**. Entrez le **Nom d'utilisateur** et le **Mot de passe** du compte domaine avec suffisamment de droits pour le client, comme l'installation dans une **Langue** définie.

Toutes les six heures (réglage par défaut), l'application G DATA ManagementServer synchronise ses données avec le serveur Active Directory. Cette valeur peut être modifiée sous **Paramètres généraux** > **Synchronisation**.

> Les changements sur Active Directory sont automatiquement synchronisés avec le ManagementServer. Cependants, si les clients changent de domaine, le lien Active Directory du groupe Management Server de l'ancien domaine doit être retiré manuellement. Après avoir attribué un élément Active Directory depuis le nouveau domaine au groupe Management Server, les clients sont automatiquement synchronisés avec le nœud approprié sous l'onglet **Clients**.

4.2.2.2. ManagementServers

Le type de ManagementServer s'affiche de la manière suivante dans la rubrique ManagementServers :

- Racine
- Serveur principal
- Serveur secondaire
- Serveur de sous-réseau

Quand un serveur est sélectionné, les **modules de serveur** correspondant sont affichés dans l'onglet module.

4.2.3. Modules

En fonction de la rubrique choisie dans **Clients/ManagementServers**, les onglets correspondants s'affichent dans la partie droite de la fenêtre. Cliquez sur l'en-tête d'un onglet pour y accéder.

La plupart des onglets disposent d'une barre d'icône qui en plus des icônes spécifiques, contient les icônes suivants :

- **Rafraîchir** : Rafraichi la vue.
- **Supprimer** : supprime l'objet sélectionné/les objets sélectionnés.
- **Imprimer** : Imprime les objets sélectionnés
- **Affichage des pages** : affiche à l'écran une prévisualisation de ce qui va être imprimé
- **Période** : Défini la période prise en compte pour l'affichage des informations

Les onglets disposent également de fonctionnalités permettant de faire les actions suivantes:

- Afin de trier une liste, cliquez sur le haut de la colonne.
- Pour ajouter/supprimer l'affichage d'une colonne pour les listes affichées, vous devez faire un clic droit sur l'en-tête d'une colonne, cliquer sur **Sélectionner les colonnes**, puis cochez/décochez en fonction des colonnes que vous souhaitez voir.
- Pour réduire le nombre d'entrées par page, sélectionnez le **Nombre maximal par page** dans le coin inférieur droit de l'interface du programme.
- Pour saisir des filtres de texte libre, cliquez sur un des boutons de filtrage au niveau des titres des colonnes et saisissez les critères de filtrage.
- Vous pouvez filtrer les éléments de la liste, mais également les classer en utilisant des groupes. Pour ce faire, faites glisser un ou plusieurs titres de colonne sur la barre au-dessus des titres pour créer un groupe à partir de la colonne. Il est possible de créer et d'imbriquer les groupes de différentes manières pour avoir des résultats différents à l'affichage.

Chaque paramétrage de module s'applique toujours aux clients, serveurs ou groupes sélectionnés dans la section **Clients/ManagementServers**. Lorsque l'objet sélectionné est un ManagementServer ou un groupe, et que les paramétrages de machines ou de sous-groupes diffèrent, les paramètres concernés sont indiqués comme tel. Lors de l'enregistrement et l'application des paramétrages, les clients ayant des paramètres différents conservent leurs paramètres spécifiques à moins que ces paramètres ne fassent parti des paramètres modifiés, auquel cas ces paramètres sont répercutés sur les objets se trouvant en dessous dans l'arborescence. Les clients et sous- groupes ayants des paramétrages différents de leur groupe sont listés par leur nom dans la section **Clients/groupes avec des paramètres différents**. Ces objets peuvent être sélectionnés pour afficher leur paramètres en cliquant sur **Afficher les paramètres** ou rétablir les paramètres du groupe en cliquant sur **Rétablir les paramètres de groupe**.

Lorsqu'un groupe contient à la fois des clients Windows, Linux et/ou Mac, les paramètres qui ne concernent pas les clients Linux ou Mac sont affichés en vert.

Les configurations modifiées ne sont sauvegardées et transférées au(x) client(s)/serveur(s) qu'après confirmation à l'aide du bouton **Appliquer**. Dans la plupart des modules, vous pouvez déterminer sous **Informations** si les modifications effectuées ont déjà été appliquées. Cliquez sur le bouton **Refuser** pour garder les paramètres actuels.

4.3. Rubrique Clients

Lorsque l'onglet **Clients** est sélectionné dans la rubrique **Clients/ManagementServers**, les onglets relatifs à cette catégorie d'objet s'affichent pour permettre la configuration des groupes et clients.

4.3.1. Tableau de bord

La rubrique Tableau de bord comporte des informations au sujet de l'état des clients du réseau. Elles apparaissent à droite de chaque entrée, sous la forme de texte, de données chiffrées ou de dates.

Sous **Statut de l'application G DATA Security**, vous pouvez définir tous les paramètres de sécurité de base pour les clients ou groupes sélectionnés dans la rubrique **Clients**.

- Si le réseau est protégé de manière optimale contre les virus informatiques, une icône verte s'affiche à gauche des entrées répertoriées ici.
- Une icône de mise en garde s'affiche pour vous indiquer qu'un composant a probablement des problèmes de sécurité (outil de surveillance désactivé ou signatures antivirus obsolètes, par exemple).
- Lorsque vous ouvrez l'interface du programme G DATA, la plupart des icônes sont brièvement affichée en mode information. Cela ne signifie pas que le réseau n'est pas protégé. Il s'agit d'une vérification interne du statut de la protection antivirus : G DATA Administrator interroge la base de données de G DATA ManagementServer.

Cliquez sur l'entrée correspondante pour exécuter directement des actions ou accéder à la rubrique de tâches concernée. Une fois la configuration d'un composant signalé par l'icône de mise en garde optimisée, l'icône verte s'affiche de nouveau dans la rubrique Statut.

La rubrique **Communication Clients / Serveur** offre une vue d'ensemble chronologique des connexions des clients avec l'application G DATA ManagementServer. Vous devez veiller à ce que tous les clients se connectent régulièrement à l'application G DATA ManagementServer. Vous devez faire particulièrement attention aux clients qui apparaissent dans la liste **Dix principaux clients - infections**, pour des raisons techniques ou à cause du comportement des utilisateurs, par exemple. L'affichage d'un ou plusieurs clients dans cette rubrique permet parfois d'attirer l'attention de l'administrateur sur d'éventuels problèmes ou d'indiquer que des mesures techniques doivent être prises. Ainsi, en cas de tentatives d'infections liées au comportement de l'utilisateur, nous vous recommandons d'utiliser le module **PolicyManager** (disponible dans la solution **G DATA Endpoint Protection Business**). L'option **Statut du rapport** présente une vue d'ensemble du nombre de tentatives d'infections, de demandes et d'erreurs au sein du réseau.

4.3.2. Clients

L'option Clients permet de vérifier que les clients fonctionnent correctement et que les signatures antivirus et les fichiers du programme sont à jour.

4.3.2.1. Vue d'ensemble

Vous disposez ici d'une vue d'ensemble de tous les clients administrés. Vous pouvez également assurer leur gestion. Grâce à la colonne **Statut de sécurité**, vous visualisez le statut actuel des clients.

Les boutons suivants vous permettent d'assurer l'administration des clients et des groupes:

- **Rafraîchir**
- **Supprimer** : vous pouvez supprimer un client de la vue d'ensemble des clients. Cette action ne désinstalle pas le client G DATA Security de la machine cliente. Elle doit être utilisée uniquement pour des machines qui ont été mises hors service ou retirées du réseau. Si un client actif est supprimé de la liste par inadvertance, il réapparaitra automatiquement lors de sa prochaine connexion au ManagementServer (attention, les paramètres spécifiques au groupe sont perdus).
- **Imprimer**
- **Affichage des pages**

 **Installer l'application G DATA Security Client**

 **Désinstaller l'application G DATA Security Client**

 **Mettre la base de données des virus à jour maintenant** : permet de mettre la base de données des virus du client à jour avec les fichiers de G DATA ManagementServer.

 **Mettre automatiquement à jour la base de données des virus** : active la mise à jour automatique de la base de données des virus. Les clients vérifient régulièrement qu'il existe des signatures antivirus à jour au niveau de l'application G DATA ManagementServer et procèdent automatiquement à la mise à jour.

 **Mettre les fichiers du programme à jour maintenant** : met les fichiers du programme à jour sur le client. Les fichiers programme du client mis à disposition par G DATA ManagementServer sont utilisés. Une fois les fichiers du programme mis à jour, il est possible qu'un redémarrage du client soit nécessaire.

 **Mettre automatiquement à jour les fichiers du programme** : active la mise à jour automatique des fichiers du programme. Les clients vérifient régulièrement qu'il existe une nouvelle version au niveau de l'application G DATA ManagementServer et procèdent automatiquement à l'actualisation.

 **Vue d'ensemble des installations**

Lorsque l'onglet Vue d'ensemble est sélectionné, l'option de menu **Clients**, s'affiche dans la barre de menu. Les actions suivantes sont disponible depuis le menu **Clients** ou un clic Droit sur un client dans la liste :

- **Installer l'application G DATA Security Client**
- **Installer l'application G DATA Security Client pour Linux**
- **Désinstaller l'application G DATA Security Client**
- **Vue d'ensemble des installations**
- **Rétablir les paramètres de groupes** : réinitialiser les paramètres de sécurité pour les clients sélectionnés selon les paramètres de groupe.
- **Déplacer le client vers** : cette fonction vous permet de placer des clients sélectionnés dans un groupe existant. Si vous sélectionnez cette option, tous les groupes existants s'affichent dans une nouvelle fenêtre. Pour placer un client dans un groupe, sélectionnez le groupe en question et cliquez sur **OK**.
- **Modifier EULA attribué** : permet d'attribuer un accord de licence d'utilisateur final défini au client sélectionné (uniquement pour les clients Android).
- **Retirer le CLUF attribué** : permet de supprimer un accord de licence d'utilisateur final attribué au client sélectionné (uniquement pour les clients Android).
- **Gestion des accords de licence d'utilisateur final**
- **Attribuer le serveur G DATA** : si vous avez la possibilité d'attribuer des clients à des serveurs de sous-réseau spécifiques via la fonction de **Serveur** > **Vue d'ensemble**, vous pouvez également exécuter cette procédure via le menu contextuel.
- **Mettre la base de données des virus à jour maintenant**
- **Mettre automatiquement à jour la base de données des virus**
- **Mettre les fichiers du programme à jour maintenant**
- **Mettre automatiquement à jour les fichiers du programme**

- **Redémarrage après la mise à jour des fichiers du programme** : indiquez ici comment le client doit réagir une fois les fichiers du programme mis à jour.
  - **Afficher la fenêtre d'informations sur le client** : informe l'utilisateur qu'il devra redémarrer son ordinateur à la prochaine occasion pour permettre l'exécution de la mise à jour.
  - **Créer un rapport** affiche, dans la rubrique **Événements de sécurité**, des informations au sujet des clients mis à jour.
  - **Procéder au redémarrage sans demander confirmation** vous permet d'exécuter automatiquement la mise à jour sur les clients, qui redémarreront de manière forcée.
- **Supprimer** (seulement depuis le menu contextuel)
- **Autoriser** (seulement depuis le menu contextuel) : Valide l'accès au ManagementServer au(x) client(s) sélectionné(s). Pour éviter les accès non autorisés au ManagementServer, les clients déployés grâce à une installation locale doivent être autorisés avant d'être en service.
- **Propriétés** (seulement depuis le menu contextuel) : Affiche les informations concernant le client sélectionné (**Généralités**, **Info réseau**, **Risques** et **Matériels**).

Installer G DATA Security Client

Sélectionnez l'option Installer l'application G DATA Security Client pour procéder à l'**installation à distance** de l'application G DATA Security Client sur tous les ordinateurs sélectionnés.

> Pour accéder aux clients désactivés, ces derniers doivent être affichés en tant qu'actifs dans la vue d'ensemble des clients. Lors de l'utilisation de la fonction Installer l'application G DATA Security Client, le programme vous signale l'existence de clients désactivés (le cas échéant) et vous permet de les afficher.

Si l'installation à distance du logiciel ne peut pas être exécutée sur les clients, vous avez la possibilité de procéder à une installation locale directement sur l'ordinateur client, à l'aide du support d'installation G DATA ou d'un paquet d'installation du client.

Désinstaller G DATA Security Client

Cette fonction envoie un ordre de désinstallation à l'application G DATA Security Client (pour Windows et Linux). Avant de lancer la désinstallation, vous pouvez sélectionner les composants que vous souhaitez conserver. Il est possible de désinstaller le logiciel client tout en conservant sur le serveur les tâches, les rapports, les messages ou les archives de sauvegarde liées à ce client. Sélectionnez les composants à supprimer et cliquez sur **OK** pour lancer la désinstallation. Vous devez redémarrer le client pour finaliser la suppression.

Il est également possible de désinstaller le client localement. Pour ce faire, il est nécessaire disposer de droits d'administrateur. Dans le répertoire %ProgramData%\G Data\client, lancez le setup.exe pour démarrer la désinstallation. Il est possible qu'un redémarrage soit demandé. Pour les clients Linux, utilisez le script gdata_uninstall.sh, se situant généralement à ce niveau : /usr/sbin/gdata_uninstall.sh.

Gestion des accords de licence d'utilisateur final

La fenêtre Gestion des accords de licence d'utilisateur final vous permet d'ajouter, de modifier et de supprimer des accords de licence d'utilisateur final pour les appareils Android. L'option correspondante du menu Clients permet d'attribuer l'accord de licence d'utilisateur adapté à chaque appareil Android pour que l'utilisateur final soit informé et accepte l'utilisation de la solution G DATA Internet Security pour Android.

Tous les accords de licence d'utilisateur final disponibles sont répertoriés dans la fenêtre Gérer les accords de licence d'utilisateur final. Cliquez sur **Ajouter** pour ajouter un accord de licence d'utilisateur final. Vous pouvez définir le **Nom**, la **Langue** et le **Contenu** de l'accord dans la fenêtre **Créer un accord de licence d'utilisateur final**. Cliquez sur **OK** pour ajouter l'accord de licence d'utilisateur final à la liste.

Pour modifier un accord de licence d'utilisateur final existant, sélectionnez-le dans la liste et cliquez sur **Modifier**. Pour supprimer un accord de licence d'utilisateur final, sélectionnez-le et cliquez sur **Supprimer**.

4.3.2.2. Logiciel

La rubrique Logiciel vous permet de contrôler l'utilisation des logiciels sur l'ensemble du réseau. Les logiciels peuvent être ajoutés à des listes blanches ou à des listes noires pour la gestion des programmes sur le réseau.

Vous pouvez configurer la vue d'ensemble à l'aide des boutons suivants :

- **Rafraîchir**
- **Imprimer**
- **Affichage des pages**
- **Afficher tout** : cette option permet d'afficher tous les logiciels installés sur les clients du réseau.
- **Afficher uniquement le logiciel sur la liste noire** : n'affiche que les logiciels qui ont été ajoutés à la liste noire.
- **Afficher uniquement les logiciels qui ne sont pas sur la liste blanche** : cette option permet d'afficher la vue d'ensemble des logiciels installés sur les clients du réseau qui n'ont pas encore été vérifiés et classés par l'administrateur réseau. Les logiciels affichés ici peuvent être placés dans la liste blanche ou la liste noire d'un clic droit.

La liste répertorie les logiciels installés sur tous les clients de la rubrique **Clients**. Pour compléter la liste blanche ou la liste noire, cliquez sur le bouton **Liste noire du réseau** ou **Liste blanche du réseau**, puis sur le bouton **Ajouter** dans la fenêtre qui s'affiche. L'option **Déterminer les propriétés** vous permet de sélectionner les programmes que vous souhaitez ajouter à une liste noire ou à une liste blanche et d'indiquer les attributs qui permettent d'identifier les programmes. Pour utiliser un attribut en tant que règle, il vous suffit de cocher la case correspondante. Vous pouvez ainsi ajouter les logiciels d'un fabricant ou certaines versions spécifiques du programme à la liste noire ou blanche. Si vous disposez des données nécessaires, vous pouvez également ajouter des logiciels à la liste noire ou blanche en saisissant directement les caractéristiques (sans passer par l'option Déterminer les propriétés).

Par défaut, l'inventaire logiciel est filtré pour afficher les applications actuellement installées. Pour afficher toutes les applications, notamment celles précédemment installées mais qui ne sont plus présentes, sélectionnez **Réinitialiser tous les filtres** pour réinitialiser le filtre.

4.3.2.3. Matériel

Vous trouverez ici des informations au sujet du matériel utilisé par les clients. Vous pouvez configurer la vue d'ensemble à l'aide des boutons suivants.

- **Rafraîchir**

Imprimer

Affichage des pages

4.3.2.4. Messages

Vous pouvez envoyer des messages individuellement à des clients ou bien à des groupes de clients. L'envoi de ces messages permet d'informer rapidement et facilement les utilisateurs. Les messages sont affichés en tant qu'informations dans la partie inférieure droite du bureau de l'ordinateur client.

Pour créer un message, il vous suffit de cliquer avec le bouton droit de la souris sur l'écran des colonnes et de sélectionner **Envoyer un message**. Dans la boîte de dialogue contextuelle qui s'affiche, vous pouvez sélectionner les clients auxquels vous souhaitez envoyer le message en cochant ou en décochant les cases.

Si vous souhaitez que le message soit uniquement envoyé à des utilisateurs spécifiques d'un client, saisissez leurs **Nom d'utilisateur**. Saisissez ensuite le message destiné aux clients dans le champ **Message** et cliquez sur le bouton **OK**.

4.3.3. Clients (iOS)

En sélectionnant un ou plusieurs client(s) iOS dans la rubrique **Clients**, l'onglet Clients n'affiche que les détails qui concernent le(s) client(s) iOS sélectionné(s):

- **Client**: Nom de l'appareil.
- **Statut de sécurité**: Affiche le statut de sécurité actuel ou un avertissement au cas où aucun **profil** n'a été assigné ou si le profil est en attente.
- **Profil**: Affiche les **profils** assignés actuellement. Sélectionnez un profil depuis la liste pour change celui-ci ou sélectionner **- Aucun profil -** pour supprimer le profil existant.
- **Dernier accès**: Horodatage de la plus récente connexion entre le client iOS et le G DATA ActionCenter.
- **IMEI**: Numéro d'identification IMEI de l'appareil.
- **Capacité**: Capacité de stockage de l'appareil en GB.
- **Version**: Numéro de la version iOS.
- **Numéro de téléphone**: Numéro de téléphone de l'appareil.
- **Courrier électronique**: L'adresse email à laquelle le lien d'installation a été envoyé.
- **Nom du produit**: Nom de produit de l'appareil.

Un clic droit sur un client permet de sélectionner les options contextuelles suivantes :

- **Retirer la gestion de l'appareil**: Désactiver Mobile Device Management sur cet appareil
- **Supprimer**: Supprimer l'appareil de la liste. Avant de supprimer l'appareil de la liste, veuillez utiliser l'option **Retirer la gestion de l'appareil** pour désactiver Mobile Device Management.
- **Envoyer de nouveau le courrier électronique pour l'activation**: Renvoie le lien d'installation aux clients ayant une installation MDM inactive ou en attente.

4.3.4. Paramètres du client

Ce module vous permet de gérer les paramètres pour chaque client ou groupe de clients. Les onglets Généralités, Outil de surveillance, Messagerie électronique, Web et AntiSpam de ce module vous

permettent d'optimiser vos clients en fonction des besoins de votre réseau et de ses utilisateurs.

4.3.4.1. Généralités

Cette rubrique vous permet de modifier les paramètres essentiels des clients sélectionnés.

G DATA Security Client
La section G DATA Security Client comprend les principales fonctionnalités du client.

- **Commentaire** : saisissez ici des informations complémentaires au sujet du client (le cas échéant).
- **Symbole dans la barre des tâches** : il est possible de choisir les sessions pour lesquelles une icône client doit s'afficher dans la barre des tâches : **Ne jamais afficher**, cette option permet de masquer l'icône client, **Afficher uniquement lors de la première session** (pour les serveurs TSE ou le changement rapide d'utilisateur Windows) ou **Toujours afficher (lors de toutes les sessions)**. Si l'icône n'est pas affichée, la fonctionnalité de Security Client est fortement limitée (par exemple, l'**Analyse d'inactivité** ne peut être utilisée et l'utilisateur n'a pas accès aux **Fonctions des clients**).
- **Attribué à** : Par défaut les clients sont attribués au ManagementServer principal. La liste déroulante affiche le ManagementServer, principale et ses serveurs de sous réseau et peut être utilisé pour attribuer rapidement un client à un serveur (de sous-réseau) spécifique.

Mises à jour
La rubrique Mises à jour vous permet de définir les paramètres de mise à jour pour les signatures antivirus et les fichiers du programme.

- **Mettre automatiquement à jour les signatures antivirus** : active la mise à jour automatique de la base de données des virus. À chaque **synchronisation**, les clients vérifient si de nouvelles signatures antivirus sont disponibles sur le ManagementServer. Si des signatures antivirus plus récentes sont présentes, celles-ci sont installées automatiquement sur le client.
- **Mettre automatiquement à jour les fichiers du programme** : active la mise à jour automatique des fichiers du programme du client. À chaque **synchronisation** les clients vérifient s'il existe des fichiers de programme plus sur le ManagementServer. Si des fichiers de programme plus récents sont disponibles, ils sont automatiquement installés sur le client. Une fois les fichiers du programme mis à jour, il est possible qu'un redémarrage du poste soit nécessaire. Selon la sélection effectuée sous **Redémarrage après la mise à jour**, l'utilisateur de l'ordinateur a la possibilité de repousser la fin de l'actualisation à plus tard.
- **Redémarrage après la mise à jour** : sélectionnez l'option **Ouvrir la fenêtre d'informations sur le client** pour informer l'utilisateur qu'il devra bientôt redémarrer son ordinateur pour permettre l'application de la mise à niveau. L'option **Créer un rapport** crée un rapport dans la rubrique **Événements de sécurité**. La fonction **Procéder au redémarrage sans demander confirmation** redémarre automatiquement l'ordinateur client, sans interroger le client.
- **Participer à l'initiative d'information relative aux logiciels malveillants afin d'améliorer le taux de détection** : Active la participation à la Malware Information Initiative. Le G DATA SecurityLabs recherche continuellement des nouvelles technologies pour protéger nos clients contre les malwares (virus, vers, et logiciels malveillants). Plus nous collectons d'informations, plus les technologies sont efficaces. Cependant, beaucoup de ces informations ne sont disponibles que sur les systèmes ayant été attaqués ou infectés. La G DATA Malware Information Initiative a été créée dans le but d'inclure ces informations aux analyses. C'est dans ce contexte que des informations relatives aux malware sont envoyées à G DATA SecurityLabs.

- **Paramètres de mise à jour de la signature** : cette option permet de définir d'où les clients reçoivent les mises à jour des signatures antivirus:
  - **Charger les mises à jour de signatures à partir du serveur de gestion** : Les clients récupèrent les mises à jour des signatures anti-virus à partir de leur ManagementServer. Ils déterminent à chaque intervalle s'il existe de nouvelles signatures.
  - **Charger les mises à jour de signatures à partir d'Internet** : les clients récupèrent les mises à jour depuis le serveur de mise à jour central de G DATA. Il est possible de planifier les mises à jour sous Paramètres et planification.
  - **Charger les mises à jour de signatures à partir d'Internet si aucune connexion au ManagementServer ne peut être établie** : Cette option est recommandée pour les postes de travail mobiles, comme des ordinateurs portables. Si le client a une connexion vers le ManagementServer, il les téléchargera à partir de celui-ci. Si non, il téléchargera les signatures antivirus automatiquement depuis le serveur de mises à jour G DATA. La mise à jour peut être planifiée sous **Paramètres et planification**.

Fonctions du client

Ces options permettent de définir les autorisations dont dispose localement l'utilisateur pour certaines fonctions du client. Il est ainsi possible d'attribuer à l'utilisateur des droits complets ou des droits très limités pour la modification des paramètres.

- **L'utilisateur peut procéder aux vérifications antivirus** : en cas de doute, l'utilisateur peut exécuter une analyse antivirus indépendamment de l'application ManagementServer (solution antivirus installée localement sur son ordinateur, par exemple). Les résultats de cette analyse antivirus sont transmis à l'application ManagementServer lors de la connexion suivante. Cette fonction permet également de procéder à des modifications dans la rubrique Analyse antivirus (paramètres locaux).
- **L'utilisateur peut charger les mises à jour des signatures** : lorsque cette fonction est activée, l'utilisateur de l'ordinateur client peut, depuis un menu contextuel, charger les signatures antivirus directement depuis Internet, même sans connexion avec l'application ManagementServer.
- **L'utilisateur peut modifier les options de l'outil de surveillance** : lorsque cette fonction est activée, l'utilisateur de l'ordinateur client a la possibilité de modifier des paramètres de la rubrique **Outil de surveillance**.
- **L'utilisateur peut modifier les options de la messagerie électronique** : lorsque cette fonction est activée, l'utilisateur de l'ordinateur client a la possibilité de modifier des paramètres des rubriques **Messagerie électronique** et **AntiSpam**.
- **L'utilisateur a le droit de modifier les options Internet** : lorsque cette fonction est activée, l'utilisateur de l'ordinateur client a la possibilité de modifier des paramètres de la rubrique **Web**.
- **L'utilisateur peut afficher la quarantaine locale** : si vous autorisez l'affichage de la quarantaine locale, l'utilisateur peut désinfecter, supprimer ou réintégrer les données identifiées comme infectées ou suspectes et mises en quarantaine. Nous attirons votre attention sur le fait que, lors de la réintégration d'un fichier mis en quarantaine, le virus n'est pas supprimé. Cette option doit donc être uniquement accessible aux utilisateurs expérimentés.
- **Protection par mot de passe pour la modification des options** : afin d'éviter toute manipulation abusive des paramètres locaux, il est possible de n'autoriser la modification des options qu'une fois un mot de passe saisi. Cela permet ainsi d'éviter qu'un utilisateur ne modifie les paramètres du client. Le mot de passe peut être attribué à un client ou un groupe, c'est

pourquoi il doit être uniquement communiqué aux utilisateurs autorisés.

Tâches d'analyse

Vous pouvez indiquer ici les éléments qui ne doivent pas être vérifiés lors de l'exécution des tâches d'analyse. Les zones d'archivage et de sauvegarde d'un disque dur ou d'une partition peuvent ainsi être définies en tant qu'exceptions, certains dossiers et certaines extensions de fichiers peuvent également être exclues des tâches d'analyse. Ces exceptions peuvent également être définies pour des groupes complets. Si les clients d'un groupe disposent de répertoires d'exception différents, vous pouvez ajouter de nouveaux répertoires ou supprimer les répertoires existants. Les répertoires spécialement définis pour les clients sont conservés. Le même processus peut être appliqué aux exceptions de l'outil de surveillance.

Analyse d'inactivité

Si vous souhaitez que le client exécute une analyse antivirus lorsque l'ordinateur est inactif, sélectionnez l'option **Analyse en cas d'inactivité activé**. Cliquez sur le bouton **Modifier** pour définir la zone d'analyse. Tous les disques durs locaux sont sélectionnés ici par défaut.

4.3.4.2. Gardien

Vous pouvez définir ici les paramètres de l'outil de surveillance. L'outil de surveillance ne doit en principe pas être désactivé, il offre en effet une protection en temps réel contre les virus. Si l'outil de surveillance est désactivé, il n'assure plus cette protection. Nous vous recommandons donc de désactiver l'outil de surveillance uniquement lorsque cela présente un intérêt certain (dépannage ou diagnostic, par exemple). Il est possible de définir des exceptions pour l'outil de surveillance. Si l'outil de surveillance nuit aux performances d'une application, vous pouvez ajouter des exceptions pour les fichiers de programme, les processus ou les fichiers correspondants. Les fichiers faisant partie des exceptions ne sont alors plus vérifiés par l'outil de surveillance. Nous attirons votre attention sur le fait que l'ajout d'exceptions à l'outil de surveillance peut présenter un risque pour la sécurité.

Paramètres

Les paramètres de l'outil de surveillance peuvent être utilisés pour configurer l'outil de surveillance et définir des exceptions.

- **Statut de l'outil de surveillance** : ici vous pouvez activer ou désactiver l'outil de surveillance. Il est conseillé de le laisser activé. Il constitue la base d'une protection contre les virus.
- **Utiliser les moteurs** : le logiciel G DATA fonctionne avec deux unités d'analyse antivirus fonctionnant indépendamment l'une de l'autre. En principe, l'utilisation des deux moteurs garantit une prévention optimale contre les virus informatiques. L'utilisation d'un seul moteur apporte en revanche des avantages en matière de performances.
- **En cas d'infection** : vous pouvez définir ici ce qui doit se passer lorsqu'un fichier infecté est détecté. Les différentes options de paramètres se justifient selon le but assigné à chaque client.
  - **Bloquer l'accès au fichier** : les fichiers infectés ne peuvent ni être lus ni être réécrits.
  - **Désinfecter et déplacer en quarantaine** : le fichier est placé en quarantaine et une tentative pour supprimer le virus est faite.
  - **Déplacer le fichier en quarantaine** : le fichier infecté est envoyé en quarantaine. Une désinfection du fichier peut alors être effectuée manuellement par l'administrateur système.
  - **Supprimer le fichier infecté** : cette mesure rigoureuse sert à endiguer efficacement le danger que représente le virus. Il peut cependant arriver que, dans de rares cas, un faux-positif entraîne la perte de données.

- **Archives infectées** : indiquez ici comment les archives infectées doivent être traitées. Lors de la définition de ces paramètres, tenez compte du fait qu'un virus à l'intérieur d'une archive ne peut causer de dommages que lorsque l'archive est ouverte.
- **Mode d'analyse** : indiquez ici comment les fichiers doivent être analysés. L'option **Accès en lecture** analyse les fichiers lors de leur lecture. L'option **Accès en lecture et en écriture** vérifie les fichiers lors de la lecture, mais également lors de l'écriture. Cette option permet de vous protéger des virus éventuellement présents sur un autre client non protégé ou provenant d'Internet. L'option **Lors de l'exécution** lance l'analyse du fichier lors de son exécution.
- **Vérifier les accès au réseau** : vous pouvez définir ici le comportement de l'outil de surveillance en ce qui concerne les accès au réseau.
- **Heuristique** : l'analyse heuristique permet de détecter les virus figurant dans les bases de données actualisées en permanence, mais également les caractéristiques types des virus. Cette méthode augmente le niveau de sécurité, mais de fausses alertes peuvent parfois être déclenchées.
- **Vérifier les archives** : l'analyse de données compressées dans des archives nécessite beaucoup de temps et s'avère généralement inutile lorsque l'outil de surveillance antivirus G DATA est actif sur le système. Lorsqu'une archive est décompressée, l'outil de surveillance reconnaît alors les virus jusqu'ici cachés et empêche automatiquement leur propagation. Pour éviter que les performances ne soient altérées par la vérification inutile de gros fichiers d'archives rarement utilisés, vous pouvez limiter la taille (exprimée en kilo-octets) des fichiers d'archives analysés.
- **Vérifier les archives de la messagerie électronique** : cette option doit théoriquement être désactivée. En effet, l'analyse des archives de courriers électroniques nécessite généralement beaucoup de temps et lorsqu'un courrier électronique infecté est détecté, la boîte aux lettres est mise en quarantaine ou supprimée, selon les paramètres de l'analyse antivirus. Les courriers présents dans l'archive ne sont alors plus disponibles. L'outil de surveillance bloque l'exécution des pièces jointes aux courriers électroniques infectés. La désactivation de cette option ne crée donc aucune faille au niveau de la sécurité. Lors de l'utilisation de l'application Outlook, les courriers entrants et sortants sont également vérifiés à l'aide d'un plug-in.
- **Vérifier les zones système au démarrage de la machine/Vérifier les zones système en cas de changement de support** : certaines zones du système (telles que les secteurs d'amorçage) de votre ordinateur ne doivent pas être exclues du contrôle antivirus. Vous pouvez définir ici si elles sont analysées lors du démarrage du système ou lors d'un changement de support de données (lors de l'insertion d'un nouveau DVD, par exemple). En règle générale, vous devez activer au moins l'une de ces deux fonctions.
- **S'assurer de l'absence de composeurs/logiciels espions/logiciels publicitaires** : le logiciel G DATA vous permet également de détecter la présence de composeurs et autres programmes malveillants (logiciels espions, logiciels publicitaires, logiciels à risques) sur votre système. Nous parlons ici de programmes qui établissent des connexions Internet payantes indésirables ou dont le potentiel nuisible n'a rien à envier à celui des virus sur le plan économique. Les logiciels espions peuvent ainsi enregistrer vos habitudes de navigation ou vos saisies au clavier (et donc vos mots de passe) à votre insu et les transmettre à des étrangers via Internet dès que l'occasion se présente.
- **Informer l'utilisateur en cas de détection de virus** : si cette option est activée, en cas de virus détecté, l'outil de surveillance ouvre une fenêtre d'avertissement sur le client concerné, afin que l'utilisateur sache qu'un virus a été détecté sur son système. Le fichier, ainsi que le chemin et la désignation du virus détecté sont affichés.

Vous pouvez limiter l'analyse antivirus à certains répertoires du client sous **Exceptions**. Vous pouvez ainsi exclure les dossiers incluant des archives rarement utilisées et les vérifier dans le cadre d'une tâche d'analyse spéciale. Le schéma d'analyse permet ainsi d'exclure certains fichiers et types de fichiers de l'analyse antivirus. Les exceptions suivantes sont possibles :

- **Répertoire** : cliquez sur les boutons du répertoire pour sélectionner un dossier (le cas échéant, les sous-dossiers présents inclus) que vous ne souhaitez pas contrôler à l'aide de l'outil de surveillance.
- **Lecteur** : sélectionnez un lecteur (partition, disque dur) que vous ne souhaitez pas contrôler à l'aide de l'outil de surveillance en cliquant sur le bouton du répertoire.
- **Fichier** : vous pouvez saisir ici le nom d'un fichier que vous ne souhaitez pas contrôler à l'aide de l'outil de surveillance. Vous pouvez utiliser des caractères génériques ici.

  Les caractères de remplacement fonctionnent comme suit : le point d'interrogation (?) remplace un caractère. L'astérisque (*) remplace des suites de caractères. Par exemple, pour exclure tous les fichiers portant l'extension .exe, vous devez saisir **.exe*. Pour exclure les fichiers de feuilles de calcul de différents formats (.xls, .xlsx, par exemple), il vous suffit de saisir **.xls?*. Pour protéger des fichiers de différents types mais dont le nom commence de la même manière, saisissez *text*.**, par exemple. Les fichiers text1.txt, text2.txt, text3.txt, etc. seront alors exclus.
- **Processus** : si un processus ne doit pas être surveillé par l'outil de surveillance, vous devez saisir le chemin du répertoire et le nom du processus ici.

Vous pouvez répéter cette opération autant de fois que nécessaire et supprimer ou modifier les exceptions existantes dans la fenêtre Exceptions de l'outil de surveillance.

Surveillance du comportement

La surveillance du comportement constitue une protection supplémentaire contre les fichiers et processus nuisibles. À la différence de l'outil de surveillance, elle ne travaille pas à partir de signatures, mais analyse le comportement réel d'un processus. Pour procéder à un classement, la surveillance du comportement se base sur différents critères dont le droit d'écriture dans le registre et la création éventuelle d'entrées de lancement automatique. Si le nombre de caractéristiques permet de conclure qu'un programme manifeste au minimum un comportement suspect, l'action définie sous **En cas de menace** est effectuée. Les options **Uniquement enregistrer dans le journal**, **Bloquer le programme** et **Bloquer le programme et le mettre en quarantaine** sont mises à votre disposition.

Chaque fois que la surveillance comportementale exécute une action, un rapport est ajouté au module **Événements de sécurité**. Si un programme a été identifié à tort comme une menace, le rapport correspondant peut être utilisé pour créer une entrée dans la liste blanche. Les entrées dans la liste blanche sont visibles et peuvent être supprimées en cliquant sur **Modifier la liste blanche à l'échelle du réseau**.

Protection anti-exploit

Les Exploits recherchent les failles de sécurité dans les logiciels d'éditeurs tiers sur le client. La Protection anti-exploit vérifie constamment le comportement des logiciels installés pour détecter les irrégularités. Si un comportement inhabituel est détecté, l'action à mener est à définir dans **En cas de détection d'un exploit** : **Uniquement enregistrer dans le protocole** ou **Empêcher l'exécution**. Lorsque **Avertir l'utilisateur lors de la détection d'un exploit** est coché, l'utilisateur est informé du comportement dangereux de ce logiciel.

Chaque fois que la Protection anti-exploit effectue une action, un rapport est ajouté au module **Événements de sécurité**. Si un programme a été identifié à tort comme une menace, le rapport correspondant peut être utilisé pour créer une entrée dans la liste blanche. Les entrées dans la liste blanche sont visibles et peuvent être supprimées en cliquant sur **Modifier la liste blanche à l'échelle du réseau**.

USB Keyboard Guard

USB Keyboard Guard protège les clients contre les attaques dîtes BadUSB. Il s'agit d'appareils reprogrammés de façon malveillantes, tels que des caméras, des clés USB ou des imprimantes, pouvant agir comme des claviers quand ils sont branchés sur un ordinateur. Pour éviter que ces appareils exécutent automatiquement des commandes non autorisées, USB Keyboard Guard demande à l'utilisateur son autorisation s'il détecte un appareil USB identifiés comme un clavier. Si l'utilisateur a en effet branché un clavier, il peut alors l'autoriser. Mais si l'appareil est identifié comme un clavier alors que l'utilisateur a branché un autre appareil, il n'est pas conseillé de l'autoriser car il pourrait être malveillant.

Un rapport sera alors ajouté dans le module **Événements de sécurité**, que l'utilisateur ait autorisé ou non l'appareil USB. Si l'appareil a été autorisé, l'administrateur peut décider de le bloquer par un clic droit sur le rapport et annuler l'autorisation.

Anti-Ransomware

Alors que les malwares classiques infectent les appareils pour en faire des botnet ou y voler des informations, les développeurs de rançongiciel essayent de gagner de l'argent en extorquant directement l'utilisateur. Pour parvenir à ses fins, les rançongiciels verrouillent le système ou chiffrent les données jusqu'à ce que la victime verse la rançon. En plus des détections par signatures et comportementales, la fonction Anti-Ransomware détecte les actions spécifiques des rançongiciels telles que le chiffrement de fichiers et les bloque avant qu'ils ne puissent faire plus de dégâts. L'action à mener en cas de détection d'un rançongiciel est définie sous : **En cas de menace**. Les choix disponibles sont **Journaliser** et **Mettre en quarantaine**. Si la case **Notifier l'utilisateur** a été coché, l'utilisateur recevra également une notification de la détection de la menace.

Lorsque la fonction Anti-Ransomware effectue une action, l'évènement est journalisé sous l'onglet **Évènements de sécurité**. L'évènement correspondant à un logiciel ayant été à tort identifié comme une menace, peut être utilisé pour ajouter ce dernier à la liste blanche. Les éléments de la liste blanche peuvent être visualissé et supprimés en cliquant sur **Modifier la liste Blanche Globale**.

4.3.4.3. Courrier électronique

Il est possible de configurer une protection antivirus spécifique à la messagerie électronique pour chaque instance G DATA Security Client. Les ports standards des protocoles POP3, IMAP et SMTP sont alors surveillés. Pour Microsoft Outlook, un plug-in spécial est utilisé. Le plug-in vérifie automatiquement tous les courriers électroniques entrants et veille à ce que des courriers électroniques infectés ne soient pas envoyés.

Courriers entrants

La rubrique Courriers entrants définit les options pour l'analyse des courriers électroniques entrants.

- **En cas d'infection** : vous pouvez définir ici ce qui doit se passer lorsqu'un fichier infecté est détecté. Les différents paramètres disponibles ici sont utiles selon le but dans lequel le client est utilisé.
- **S'assurer de l'absence de virus dans les courriers reçus** : lorsque cette option est activée,

l'ensemble des courriers électroniques qui parviennent au client est analysé.

- **Vérifier les courriers non lus au démarrage du programme (Microsoft Outlook uniquement)** : cette option permet de s'assurer de l'absence de virus au niveau des courriers électroniques que reçoit le client lorsqu'il n'est pas connecté à Internet. À l'ouverture de l'application Outlook, tous les messages non lus dans le dossier Boîte de réception et ses sous-dossiers sont analysés.
- **Joindre le rapport au courrier infecté reçu** : lorsqu'un courrier électronique reçu par le client contient un virus, le corps de ce courrier électronique comprend, sous le texte du courrier, le message suivant : *ATTENTION ! Ce message contient le virus suivant*, suivi du nom du virus. L'objet est également précédé de la mention *[VIRUS]*. Si vous avez activé l'option **Supprimer la pièce jointe/le texte**, le système vous informe également que la section infectée du courrier électronique a été supprimée.

Courriers sortants

La rubrique Courriers sortants définit les options pour l'analyse des courriers électroniques sortants.

- **Vérifier les courriers avant envoi** : afin que vous ne transmettiez aucun virus depuis votre réseau, le logiciel G DATA vous offre également la possibilité de vous assurer de l'absence de virus dans vos courriers avant envoi. Si vous êtes sur le point d'envoyer un virus, le message *Le courriel [ligne d'objet] contient le virus suivant : [Nom du virus]*. Le courrier électronique correspondant n'a pas été envoyé.
- **Joindre le rapport au courrier sortant** : un rapport d'analyse est ajouté au corps de chaque courrier sortant, après le corps de texte du courrier. Il est intitulé *Recherche des virus effectuée par G DATA AntiVirus*tant que l'option **Vérifier les courriers avant envoi** est activée. Vous pouvez également indiquer ici la date de la version du logiciel G DATA AntiVirus (Informations relatives à la version).

Options d'analyse

La rubrique Options d'analyse définit les paramètres d'analyse pour les courriers électroniques entrants et sortants.

- **Utiliser les moteurs** : le logiciel G DATA fonctionne avec deux unités d'analyse antivirus fonctionnant indépendamment l'une de l'autre, appelées moteurs. L'utilisation des deux moteurs garantit des résultats optimaux dans le cadre de la lutte antivirus. L'utilisation d'un seul moteur, par contre, améliore les performances ; autrement dit, une analyse peut être plus rapide si vous n'utilisez qu'un moteur.
- **OutbreakShield** : la technologie OutbreakShield permet de détecter et de combattre les programmes malveillants dans les envois massifs de messages électroniques avant que les signatures antivirus correspondantes ne soient disponibles. Selon une multitude de critères, les courriers dangereux sont identifiés et bloqués ce qui lui permet de combler en temps réel le laps de temps entre le début d'un envoi massif de messages électroniques infectés et son traitement au moyen de signatures adaptées. L'option **Modifier** vous permet de définir si OutbreakShield utilise des signatures supplémentaires afin d'améliorer la qualité de la reconnaissance. Vous pouvez également saisir ici les codes d'accès pour la connexion à Internet ou un serveur proxy, permettant à OutbreakShield d'effectuer un téléchargement automatique des signatures à partir d'Internet.

Messages d'avertissement

La rubrique Messages d'avertissement configure les messages d'avertissement pour les courriers électroniques infectés reçus par le destinataire.

- **Informer l'utilisateur en cas de détection de virus** : vous pouvez automatiquement informer le destinataire qu'un message est infecté. Une notification du virus est alors affichée sur son bureau.

Protection Outlook

Le module Protection Outlook permet de procéder à des analyses de courriers électroniques dans Outlook à l'aide d'un plug-in.

- **Protéger Microsoft Outlook à l'aide d'un plug-in** : l'activation de cette fonction entraîne l'ajout de la fonction **Rechercher des virus dans un dossier** dans le menu **Outils** du programme Outlook du client. Quels que soient les paramètres de l'application G DATA Administrator, l'utilisateur de chaque client peut analyser le dossier de courriers électroniques sélectionné. Dans la fenêtre d'aperçu des messages, vous pouvez procéder à l'analyse des pièces jointes à l'aide de la fonction **Rechercher des virus dans un courrier** du menu **Outils**. Une fois le processus terminé, un écran d'informations détaillant les résultats de l'analyse s'affiche. Vous saurez si l'analyse a été effectuée dans son intégralité et recevrez des informations détaillées sur les courriers électroniques et pièces jointes analysés, les erreurs de lecture éventuelles, ainsi que les virus détectés et ce qu'il en est advenu. Les deux fenêtres peuvent être masquées par la commande **Fermer**.

Surveillance des ports

Les ports standard POP3 (110), IMAP (143) et SMTP (25) sont généralement surveillés. Si les paramètres des ports sont différents, vous pouvez adapter la surveillance en fonction.

4.3.4.4. Web

Cette rubrique vous permet de définir les paramètres d'analyse pour Internet et les opérations bancaires en ligne. Si vous ne souhaitez pas procéder à la vérification du contenu Internet, l'**Outil de surveillance** intervient en cas d'accès à des fichiers téléchargés infectés. Le système du client correspondant reste donc protégé sans analyse des contenus Internet tant que l'outil de surveillance antivirus est activé.

Contenus Internet (HTTP)

La rubrique Contenus Internet (HTTP) traite les paramètres d'analyse pour le flux de données HTTP.

- **Traiter les contenus Internet (HTTP)** : les options Web vous permettent d'activer l'analyse antivirus de tous les contenus HTTP lors de la navigation. Les contenus Web infectés ne sont pas exécutés et les pages correspondantes ne sont pas affichées. Si un proxy est utilisé au niveau du réseau pour l'accès à Internet, le port du serveur utilisant le proxy doit être saisi. Sinon, le contrôle du trafic Internet est impossible. Le **Contrôle du contenu Web** (disponible dans la version G DATA Endpoint Protection Business) utilise également ces paramètres.
- **Éviter les dépassements de temps dans le navigateur** : étant donné que le logiciel G DATA traite les contenus Web avant leur affichage dans le navigateur Internet, ce qui peut nécessiter un certain temps selon le chargement de données, un message d'erreur peut apparaître dans le navigateur Internet s'il ne reçoit pas les données demandées de suite, car elles doivent d'abord faire l'objet d'une analyse par le logiciel antivirus à la recherche de routines préjudiciables. Si vous cochez la case Éviter les dépassements de temps dans le navigateur, ce message d'erreur

est bloqué. Les données du navigateur Internet apparaissent tout à fait normalement une fois l'analyse antivirus effectuée.

- **Limitation de la taille pour les téléchargements** : vous pouvez interrompre l'analyse HTTP des contenus trop volumineux. Les contenus des pages seront analysés par l'outil de surveillance antivirus si des routines nuisibles s'activent. La limitation de la taille présente l'avantage d'empêcher le ralentissement causé par les contrôles antivirus lors du téléchargement de fichiers volumineux.
- **Exceptions à la protection Web à l'échelle du réseau** : cette fonction vous permet d'exclure certains sites Internet du contrôle effectué par la protection Internet.

BankGuard
Les chevaux de Troie bancaires constituent une menace grandissante, cependant la technologie de G DATA BankGuard protège vos opérations bancaires. La vérification de l'authenticité des bibliothèques réseau utilisées permet à la technologie G DATA BankGuard de s'assurer que votre navigateur Internet n'est pas manipulé par un cheval de Troie bancaire. Cette protection immédiate proactive à plus de 99 % permet de sécuriser les opérations bancaires en ligne de manière optimale, même contre des chevaux de Troie encore inconnus. La fonction BankGuard doit être activée pour tous les clients qui utilisent Internet Explorer, Firefox et/ou Chrome.

4.3.4.5. AntiSpam

Le module AntiSpam est disponible dans les **solutions** Client Security Business, Endpoint Protection Business et Managed Endpoint Security.

Si vous cochez la case **Utiliser le filtre AntiSpam**, le trafic de courriers du client fait l'objet de tests pour détecter les éventuels spams. Lorsqu'un courrier électronique est détecté en tant que spam ou en cas de suspicion de spam, vous pouvez configurer un message d'avertissement qui sera affiché dans le champ d'objet du courrier.

> Si le **plugin Microsoft Outlook** a été mis en fonction, les spams entrants seront déplacés vers le dossier AntiSpam. Pour les autres clients de messagerie, les spams peuvent automatiquement être déplacés vers un dossier spam dédié en définissant une règle de filtrage qui laisse apparaître l'avertissement spam dans le sujet. Pour configurer les paramètres AntiSpam en utilisant Microsoft Exchange, veuillez-vous référer à **Paramètres Exchange** > **AntiSpam**.

4.3.5. Paramètres Exchange

G DATA Exchange Mail Security est un **module optionnel**.

Le menu de paramétrage Exchange permet de configurer le plugin G DATA MailSecurity Exchange. Le module est disponible s'il est installé sur un serveur Exchange 2007 SP1, 2010 ou 2013.

4.3.5.1. Généralités

La section Généralités permet de configurer les mises à jour, la protection contre les logiciels malveillants et les paramètres d'analyse pour le plugin Exchange de MailSecurity.

Mettre automatiquement à jour les signatures antivirus
Comme les autres clients, les clients Exchange peuvent être mis à jour automatiquement :

- **Mettre automatiquement à jour les signatures antivirus** : active la mise à jour automatique de la base de données des virus. Les clients s'assurent à chaque **synchronisation** qu'il a des

signatures antivirus à jour au niveau de l'application ManagementServer. Si des signatures antivirus plus récentes sont présentes, celles-ci sont installées automatiquement sur le client.

- **Mettre automatiquement à jour les fichiers du programme** : active la mise à jour automatique des fichiers du programme du client. Les clients vérifient à chaque **synchronisation** s'il existe des fichiers de programme plus récents au niveau de l'application ManagementServer. Si des fichiers de programme plus récents sont disponibles, ils sont automatiquement installés sur le client.

Antivirus protection
Activez la protection antivirus en cochant **Analyse lors de l'accès**. L'Analyse lors de l'accès analyse tous les emails, pièces jointes et autres objets sitôt qu'ils sont envoyés ou reçus. Si un contenu malveillant est trouvé, les actions définies dans la section **Paramètres d'analyse** sont mises en œuvre.

Paramètres d'analyse
Les paramètres d'analyse sont semblables à ceux utilisés pour l'**Outil de surveillance** et les **Tâches d'analyse**.

- **Utiliser les moteurs** : Paramétrage du nombre de moteurs à utiliser. Les paramètres recommandés sont les deux moteurs.
- **En cas d'infection** : Comme le **Gardien**, le plugin Exchange peut effectuer l'action définie ici lorsqu'un code malveillant est découvert.
- **Types de fichiers** : Pour augmenter la vitesse d'analyse, les analyses peuvent être limitées au fichier exécutable et aux documents, cependant il est recommandé d'analyser tous les fichiers.
- **Utiliser l'heuristique** : Cette fonctionnalité active la détection de code malveillant basée sur des caractéristiques typiques des codes malveillants.
- **Vérifier l'archive** : Les fichiers archives peuvent être analysés pour trouver d'éventuels codes malveillants. Si des codes malveillants sont trouvés, alors le fichier archive complet sera désinfecté ou supprimé. Si vous avez configuré la mise en quarantaine, l'email complet ('archive incluse) sera mis en quarantaine.

4.3.5.2. AntiSpam

Grâce à l'option AntiSpam du plugin Exchange, vous êtes sûr que les spams sont filtrés avant qu'ils n'atteignent le destinataire. Ce n'est disponible que sur les serveurs Exchange qui fonctionnent avec le rôle Transport Hub.

Les messages spams sont classés en trois catégories: **Suspicion de spam**, **Probabilité élevée de spam** et **Probabilité très élevée de spam**. Pour chaque catégorie, il est possible de personnaliser l'action du plugin Exchange :

- **Réaction**
  - **Distribuer le courrier électronique** : Cet email sera délivré à son destinataire.
  - **Placer le courrier électronique en quarantaine** : Cet email va être déplacé vers le dossier de quarantaine.
  - **Rejeter le courrier électronique** : Cet email sera rejeté.
  - **Placer le courrier électronique dans le dossier du spam** : Cet email sera déplacé vers le dossier spam.
- **Préfixe dans la ligne d'objet** : ajouter un préfixe à la ligne d'objet de l'email, tel que *[SPAM?]*.

- **Notification dans le texte** : ajouter du texte au corps de l'email.
- **Créer des rapports** : ajouter un rapport dans le module des **Événements de sécurité**.

En plus des trois catégories de spams, vous pouvez définir une liste blanche et une liste noire comprenant des adresses emails ou des domaines. Les emails provenant d'adresses ou de domaines sur la liste blanche ne seront jamais vérifiés en tant que spam ; les adresses et les domaines sur la liste noire seront toujours traités selon la configuration de la **Probabilité très élevée de spam**. La liste Blanche/Noire peut être Importée/exportée via un fichier .json.

4.3.6. Paramètres Android

L'onglet Paramètres Android permet d'accéder facilement aux options de gestion des appareils Android.

4.3.6.1. Généralités

L'onglet Généralités propose des paramètres pour les mises à jour automatiques, la protection Web, l'analyse antivirus et la synchronisation, ainsi que deux options pour la gestion des périphériques :

- **Description** : saisissez ici des informations complémentaires au sujet du client (le cas échéant).
- **Nom de l'appareil** : saisissez ici le nom du périphérique.

Mises à jour

La section Mises à jour comprend les paramètres relatifs aux mises à jour.

- **Automatique** : vous pouvez déterminer ici si le client Android doit rechercher automatiquement les signatures de logiciels et les signatures antivirus. Si les mises à jour ne sont pas téléchargées automatiquement, l'utilisateur peut procéder à l'actualisation manuellement. Si vous optez pour une mise à jour automatique, vous pouvez définir la fréquence de mise à jour et indiquer si l'actualisation doit avoir lieu via le réseau mobile ou uniquement via le réseau local sans fil.

Protection Web

La rubrique Protection Web bloque l'ouverture des sites internet d'hameçonnage dans les navigateurs Android et Chrome. Depuis que le trafic de donnée est nécessaire pour vérifier la liste des sites internet d'hameçonnage, la protection web peut être configurée pour ne rechercher les sites internet que lors d'une connexion Wi-Fi. La rubrique Protection Web permet par conséquent de limiter la protection Web aux réseaux locaux sans fil.

- **Activé** : indiquez ici si les périphériques Android doivent être protégés par le module Protection Web lors de l'accès à Internet. Cette option peut être configurée en tant que protection générale ou uniquement en cas d'accès via le réseau local sans fil.

Vérification antivirus

La rubrique Vérification antivirus vous permet de définir les paramètres pour les analyses antivirus à la demande et en cas d'accès.

- **Lors de l'installation d'Apps** : vous pouvez déterminer ici que les applications doivent être automatiquement vérifiées lors de leur installation.
- **Périodique** : vous pouvez définir ici une analyse périodique. Pour ce faire, cochez la case Périodique et définissez ensuite la **Fréquence**.
- **Mode d'économie d'énergie** : interrompez les analyses périodiques lorsque le smartphone fonctionne en mode économie d'énergie.

- **Uniquement durant la charge** : vous pouvez indiquer ici que l'analyse périodique ne doit avoir lieu que lorsque l'appareil mobile est en cours de chargement.
- **Type** : vous pouvez indiquer ici si l'analyse doit porter sur le **Système (analyse complète)** ou uniquement sur les **Applications installées**.

Synchronisation
L'option Synchronisation définit la fréquence à laquelle le client Android synchronise ses données avec l'application ManagementServer. Saisissez le cycle d'actualisation en heures et déterminez si les synchronisations peuvent uniquement avoir lieu via le réseau local sans fil ou également via le réseau téléphonique.

4.3.6.2. Politiques

Vous avez la possibilité de définir des politiques pour différents types de téléphones portables et de protéger ainsi le réseau de votre entreprise.

Paramètres généraux
Sélectionnez le **Type de téléphone** correspondant à l'appareil sélectionné. Vous décidez alors des différents paramétrages pour l'utilisateur de G DATA Internet Security pour Android :

- **Professionnel** : G DATA Internet Security pour Android utilise les paramètres du profil professionnel qui est synchronisé régulièrement avec G DATA ManagementServer. L'utilisateur n'a pas l'autorisation d'accéder aux paramètres. C'est un paramétrage recommandé pour les appareils professionnels.
- **Privé** : G DATA Internet Security pour Android utilise les paramètres du profil privé, qui n'est pas synchronisé avec G DATA ManagementServer. L'utilisateur a l'autorisation d'accéder à tous les paramètres de G DATA Internet Security pour Android.
- **Mixte :** L'utilisateur peut passer librement d'un profil professionnel à un profil privé.

> Attention : Quand le mode **Privé** ou **Mixte** est activé, l'utilisateur aura accès aux fonctionnalités qui ne peuvent être gérées de façon centralisée. Utiliser le mode **Professionnel** est recommandé pour tous les appareils Android gérés.

Indépendamment du type de téléphone, les fonctions suivantes peuvent être gérées :

- **Autoriser l'accès à la caméra (Android version 4.0 ou supérieure)** : permet de désactiver l'accès à la caméra de l'appareil photo (Android version 4.0 ou supérieure).
- **Chiffrement nécessaire (Android version 3.0 ou supérieure)** : cette option permet d'activer le chiffrement complet du périphérique (Android version 3.0 ou supérieure).
- **Autoriser les périphériques rootés** : permet d'autoriser les périphériques rootés. Lorsque cette fonction est désactivée, les périphériques rootés sont bloqués par un mot de passe d'assistance à distance défini dans **Perte /vol**. De plus, les périphériques rootés ne pourront pas accéder au réseau sans fil défini dans **Autoriser l'accès au réseau local sans fil si les conditions sont remplies**.

Autoriser l'accès au réseau local sans fil si les conditions sont remplies
Pour les périphériques rootés, l'accès à un réseau sans fil défini peut être bloqué. Cela restreint l'accès au réseau local sans fil de l'entreprise uniquement aux périphériques qui répondent aux directives de l'entreprise.

Saisissez le **SSID** du réseau d'entreprise pour lequel l'accès doit être activé. Si le réseau est chiffré, entrez le **Mot de passe** et le type de **Chiffrement**.

4.3.6.3. Perte /vol

L'onglet Perte /vol propose différentes mesures, qui peuvent être activées à distance par SMS, pour protéger les périphériques mobiles perdus ou volés. Les périphériques volés ou perdus peuvent ainsi être bloqués, effacés ou localisés à distance. Un SMS avec les commandes correspondantes est alors envoyé au périphérique perdu depuis un numéro de téléphone digne de confiance. La fonction Firebase Cloud Messaging permet également d'activer manuellement à tout moment ces fonctions de protection contre le vol.

Vous devez définir quelques paramètres généraux avant de définir les mesures de protection contre le vol. Le **Mot de passe d'assistance à distance** est composé de nombres et fonctionne comme un code PIN. Lors de l'envoi d'une commande SMS à un appareil, le mot de passe est à inclure pour s'assurer que seul l'utilisateur autorisé peut envoyer des commandes. La commande pour redéfinir à distance le mot de passe de maintenance peut uniquement être envoyé via le **Numéro de téléphone digne de confiance**. Certaines des **Commandes SMS** déclenchent un rapport ou une notification qui sont envoyés à l'appareil à partir duquel la commande a été envoyée. Ils peuvent également, de façon alternative, être envoyés à l'**Adresse électronique pour les notifications**. Si vous activez une ou plusieurs options de **Détection de vol**, toute information disponible sur la localisation sera envoyée à cette adresse électronique.

Commandes SMS
Vous pouvez définir ici les actions exécutées par votre smartphone lorsque vous lui envoyez une commande par SMS. Cochez les cases qui correspondent aux fonctions que vous souhaitez activer :

- **Localiser l'appareil** : L'appareil enverra sa position via sms. Si une adresse email a été entrée sous **Perte /vol**, les données de localisation seront envoyées à cette adresse. Pour déclencher cette fonction, envoyez *mot de passe***locate** par SMS.
- **Supprimer les données personnelles** : cette option vous permet de réinitialiser totalement le téléphone portable volé/perdu. Toutes les données personnelles sont alors supprimées. Pour déclencher cette fonction, envoyez *mot de passe***wipe** par SMS.
- **Faire sonner** : cette fonction vous permet d'émettre un signal sonore jusqu'au lancement de l'application Internet Security pour Android. Cela permet de retrouver plus facilement un téléphone portable perdu. Pour déclencher cette fonction, envoyez *mot de passe***ring** par SMS.
- **Mettre le périphérique en sourdine** : si vous ne souhaitez pas que votre smartphone volé/ perdu puisse être détecté par l'émission de sonneries ou de sons système, vous pouvez le mettre en sourdine à l'aide de cette option. Le déclenchement du signal sonore permettant de retrouver le périphérique n'est bien évidemment pas affecté. Pour déclencher cette fonction, envoyez *mot de passe***mute** par SMS.
- **Verrouiller l'écran** : cette option vous permet de bloquer l'écran du smartphone volé/perdu. Il n'est alors plus possible de l'utiliser. Pour déclencher cette fonction, envoyez mot de passe lock par SMS. Si aucun mot de passe n'est saisi, le mot de passe que vous avez défini dans la rubrique **Perte /vol** est utilisé.
- **Définir le mot de passe pour le verrouillage d'écran** : configure un mot de passe pour déverrouiller l'appareil après l'envoi de la commande lock. Pour déclencher cette fonction, envoyez par SMS mot de passe **set device password:** *mot de passe de l'appareil*.

Pour modifier à distance le mot de passe de maintenance à distance, envoyez un SMS au téléphone portable dont le numéro est saisi sous **Numéro de téléphone digne de confiance**. La commande est la suivante : **remote password reset:** *nouveau mot de passe*.

Détection de vol
Lors de l'installation de l'application Internet Security, celle-ci identifie la carte SIM présente dans le périphérique mobile au moment de l'installation. En cas de changement de cette carte (vol ou revente du périphérique, par exemple), certaines actions peuvent être automatiquement exécutées :

- **Verrouiller l'écran** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Localiser l'appareil** : mêmes fonctionnalités que les options sous **Commandes SMS**.

Fonction d'urgence
Le framework Internet Firebase Cloud Messaging permet de déclencher des mesures d'urgence sur l'appareil Android. Ces mesures peuvent également être appliquées lorsque l'appareil est utilisé sans carte SIM. Vous devez toutefois configurer l'application Firebase Cloud Messaging au préalable : sous **Paramètres généraux** > **Android**, avant d'utiliser les functions d'urgence.

Sélectionnez ensuite les actions souhaitées et cliquez sur **Exécuter la fonction** pour envoyer la commande pour l'action au périphérique mobile :

- **Localiser l'appareil** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Mettre le périphérique en sourdine** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Faire sonner** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Définir le code PIN suivant pour le verrouillage d'écran** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Activer le verrouillage d'écran avec un code PIN** : mêmes fonctionnalités que les options sous **Commandes SMS**.
- **Rétablir les paramètres d'usine du périphérique** : mêmes fonctionnalités que les options sous **Commandes SMS**.

4.3.6.4. Applications

Le panneau Applications vous permet d'accéder à la gestion des applications de votre périphérique mobile. Pour bloquer ou autoriser des applications, vous devez d'abord déterminer si le filtre des applications doit être utilisé en mode **Liste noire** ou **Liste blanche**. En mode Liste noire, les applications répertoriées dans les listes noires sont bloquées ou leur accès est limité à l'aide d'un mot de passe. Les autres applications peuvent être utilisées. En mode Liste blanche, seules les applications se trouvant sur les listes blanches sont autorisées. Le mot de passe (code PIN) permet d'accéder aux applications bloquées. Vous pouvez également définir une **Adresse électronique pour la récupération** à laquelle le mot de passe doit être envoyé en cas d'oubli.

Toutes les applications installées sur le périphérique mobile sont répertoriées sous **Applications disponibles**. Pour chaque application, le **Nom** de l'application, la **Version** et la **Taille** sont affichés. Les boutons fléchés permettent de déplacer les applications entre la liste blanche et la liste noire. Une fois encore, vous pouvez utiliser la **Protection par mot de passe** pour les applications répertoriées.

4.3.6.5. Répertoire

Le panneau Répertoire permet la gestion complète des contacts. Les contacts peuvent être ajoutés à un répertoire dans l'application Internet Security. Ainsi, ces contacts et leurs communications peuvent être masqués sur le périphérique mobile de manière à ce qu'ils ne soient pas visibles dans le carnet d'adresses et le répertoire standard. Le répertoire de l'application Internet Security peut également totalement remplacer le répertoire officiel du système Android.

La liste principale affiche tous les contacts ajoutés au répertoire de l'application Internet Security. Pour chaque contact, le **Prénom**, le **Nom**, le ou les **Numéro(s) de téléphone** et l'**Adresse** sont affichés. Le menu déroulant **Visibilité** vous permet d'indiquer si les contacts doivent être affichés (**Visible**) ou non (**Masqué**) dans le répertoire Android standard. Vous pouvez également masquer tous les appels et SMS des contacts correspondants à l'aide de l'option **Communication masquée**. Pour ajouter un contact au répertoire, cliquez sur **Ajouter une entrée**. La fenêtre **Base de données des contacts** affiche tous les contacts définis. Sélectionnez un ou plusieurs contacts et cliquez sur **Sélectionner** pour ajouter les contacts au répertoire. Pour supprimer un contact du répertoire, cliquez sur **Supprimer une entrée**.

Pour ajouter un contact à la base de données des contacts, cliquez sur le bouton **Créer un contact** dans la barre d'icônes. L'option **Importer les contacts** permet d'importer des contacts de l'unité organisationnelle Active Directory. Lors de la création d'un contact, vous devez indiquer au moins un **Prénom** ou un **Nom**. Vous pouvez également ajouter une ou plusieurs adresses postales, ainsi que des adresses électroniques, des numéros de téléphone, des numéros de fax et des organisations. Pour supprimer un contact de la base de données de contacts, sélectionnez le contact et cliquez sur l'icône **Supprimer** dans la barre d'icônes ou sélectionnez l'option **Supprimer** dans le menu contextuel.

4.3.6.6. Appels / SMS

Le filtre d'appels vous permet de filtrer les SMS, les appels entrants et les appels sortants. Vous pouvez facilement, à l'aide de la même base de données que celle utilisée au niveau du panneau **Répertoire**, ajouter des contacts à une liste noire ou blanche ainsi que définir des filtres généraux.

Appels/SMS entrants

Dans la rubrique Appels/SMS entrants, vous pouvez définir le comportement de l'application Internet Security avec les communications entrantes. Désactivez l'option **Autoriser les appels de numéros anonymes en dépit du filtre** pour bloquer tous les appels anonymes. En sélectionnant l'option **Ajouter tous les numéros du répertoire**, les appels ou SMS entrants provenant des contacts du répertoire Android ou d'Internet Security sont autorisés en plus de ceux qui sont dans la liste blanche.

La fonction **Mode de filtrage** vous permet de définir certaines mesures pour les appels et les SMS entrants. Sélectionnez l'option **Liste noire** pour autoriser la communication avec tous les contacts, à l'exception de ceux qui se trouvent sur la liste noire, ou sélectionnez l'option **Liste blanche** pour autoriser uniquement la communication avec les contacts répertoriés dans la liste blanche. Cliquez sur **Ajouter une entrée** pour ajouter chaque contact de la base de données de contacts à la liste correspondante et sur **Supprimer une entrée** pour supprimer des entrées de la liste.

Appels sortants

Dans la rubrique Appels sortants, vous pouvez indiquer comment l'application Internet Security doit traiter les appels sortants. En sélectionnant l'option **Ajouter tous les numéros du répertoire**, vous restreignez les appels sortants aux contacts des répertoires Android ou Internet Security en plus de ceux qui sont dans la liste blanche.

La fonction **Mode de filtrage** vous permet de définir certaines mesures pour les appels et les SMS sortants. Sélectionnez l'option **Liste noire** pour autoriser la communication avec tous les contacts, à l'exception de ceux qui se trouvent sur la liste noire, ou sélectionnez l'option **Liste blanche** pour autoriser uniquement la communication avec les contacts répertoriés dans la liste blanche. Cliquez sur **Ajouter une entrée** pour ajouter chaque contact de la base de données de contacts à la liste correspondante et sur **Supprimer une entrée** pour supprimer des entrées de la liste.

Si un utilisateur tente de contacter un numéro bloqué, il est informé du blocage et il a la possibilité de demander à ce que le numéro soit débloqué. Cette procédure entraîne la création d'un rapport dans le module **Événements de sécurité**, via lequel l'administrateur peut directement créer une entrée dans la liste noire ou la liste blanche.

4.3.7. Paramètres iOS

Le menu des paramètres iOS donne accès facilement à la gestion G DATA Administrator des iOS.

4.3.7.1. Généralités

En utilisant l'onglet Généralités, vous pouvez entrer un commentaire pour les clients sélectionnés et assigner un profil :

- **Description**: Entrez un commentaire, par exemple des informations sur l'appareil ou sur sa configuration. Le commentaire n'est affiché que dans G DATA Administrator.
- **Profil activé**: Affiche le **profil** actuellement assignés. Sélectionnez un profil à partir de la liste pour le modifier ou sélectionnez **- Aucun profil -** pour supprimer le profil actuel.

En plus des commentaires et des paramètres profils, l'onglet Généralités affiche les paramètres qui ont été configures lors de l'envoi du lien par Device Management. Cela inclut le nom dans Device Management, la description, l'organisation et le Contrat de Licence de l'Utilisateur Final.

4.3.7.2. Profils

En utilisant les profils, vous pouvez déployer des politiques de sécurité aux (groups d') appareils iOS. Utilisez le bouton Ajouter un profil, de la barre d'outils, pour définir un nouveau profil, entrer son **Nom** et une **Description** (facultatif). Chaque profil peut contenir jusqu'à cinq politiques, chacune se référant à une branche spécifique de paramètres. Sous **Ajouter une politique**, sélectionnez une des cinq politiques suivantes et cliquez sur le signe Plus pour l'ajouter au profil :

- **Limitations de la fonctionnalité**: Désactive des fonctions spécifiques de l'appareil iOS (comme l'usage d'une caméra, Siri ou iCloud).
- **Limitations de l'application**: Désactive des applications spécifiques ou des paramètres d'applications (comme YouTube, iTunes Store ou Safari).
- **Limitations pour les contenus multimédias**: Désactive le contenu multimédia, en se basant sur un système de de classifications.
- **Paramètres du code**: Impose les caractéristiques de mot de passe iOS (tels que longueur minimum, complexité minimum et nombre maximum de tentatives de connexion).
- **Réseau local sans fil**: Autorise les appareils iOS à se connecter à un réseau sans fil spécifique.

Sélectionnez une politique pour éditer ces paramètres. Cliquez sur **Appliquer** pour sauvegarder le profil et ses politiques. Si vous éditez un profil qui a déjà été assigné à un appareil, le profil mise à jour sera synchronisé avec l'appareil et un rapport sera ajouté au module **Protocoles** (iOS) aussitôt que

l'appareil l'aura appliqué.

Des profils peuvent être importés ou exportés en cliquant sur les boutons correspondants. Les configurations des profils sont sauvegardées dans un fichier JSON.

4.3.7.3. Antivol

Le menu Antivol permet de déclencher une des trois actions antivol sur les appareils iOS sélectionnés :

- **Bloquer le périphérique**: L'écran de verrouillage de l'appareil sera activé (incluant un mot de passe de protection si celui-ci a été paramétré).
- **Rétablir les paramètres d'usine du périphérique**: L'appareil sera réinitialisé. Attention : Cela supprime toutes les données et désactive Device Management.
- **Supprimer le blocage par mot de passe**: Le mot de passe de l'appareil sera supprimé.

Cliquez sur **Exécuter la fonction** pour déclencher l'action sélectionnée. Le statut sera indiqué sous **Protocoles** (iOS).

4.3.8. Sendmail/Postfix

Le module Linux Mail Security Gateway est un **module optionnel**.

Cet onglet permet de configurer les paramètres du module Linux Mail Security Gateway pour les clients Linux.

4.3.8.1. Paramètres

La protection antivirus est configurée dans la partie Paramètres :

- **Réaction** : définit la réaction face aux emails infectés (**Supprimer la pièce jointe infectée**, **Placer l'e-mail en quarantaine**).
- **Préfixe dans l'objet** : ajoute un préfixe dans le champ objet de l'e-mail (ex : *[Virus]*).
- **Message dans le corps de l'email** : ajoute un message texte dans le corps de l'e-mail (ex : *Cet e-mail contient un malware*).

4.3.8.2. AntiSpam

Lorsque les paramètres AntiSpam sont utilisés, le module Linux Mail Security Gateway filtre automatiquement les emails entrants et détecte les spams.

Les spams sont rangés en trois catégories : **Suspicion de spam**, **Haute probabilité de Spam**, **Très grande probabilité de spam**. L'action à effectuer peut être personnalisée pour chaque catégorie :

- **Réaction** :
  - **Délivrer l'e-mail** : l'e-mail sera transmis à son destinataire.
  - **Supprimer le message** : l'e-mail sera supprimé.
- **Préfixe dans l'objet** : ajoute un préfixe dans le champ objet de l'e-mail.
- **Message dans le corps de l'email** : ajoute un message texte dans le corps de l'e-mail.
- **Générer un rapport** : génère une entrée dans **Événements de sécurité** lors de la détection d'un malware.

En plus des trois catégories disponibles vous pouvez définir une liste blanche et une liste noire. Les e-

mails en provenance des adresses ou domaine de la liste blanche ne seront jamais analysé contre le spam. Les e-mails provenance des adresses IP ou domaines de la liste noire sont systématiquement considéré comme Très grande probabilité de spam et sont donc traité comme tel. La liste Blanche/ Noire peut être importée/exportée via un fichier .json.

4.3.9. Squid

Le module Linux Web Security Gateway est un **module optionnel**.

L'onglet Squid permet de configurer le module Linux Web Security Gateway. Les paramètres suivants se configurent dans **Protection antivirus** :

- **Activer** : active la protection antivirus pour Squid.
- **Utiliser l'Antiphishing** : active la partie analyse cloud pour augmenter le taux de détection.
- **Générer rapports** : génère une entrée dans **Événements de sécurité** lors de la détection d'un malware.

Pour ajouter un **Domaine**, une **Adresse IP de Proxy client** ou encore un **Type MIME**, cliquer sur **Ajouter** dans **Liste noire**. Les objets se trouvant dans la liste noire sont systématiquement bloqués.

4.3.10. Tâches

Dans cette rubrique Tâches, vous pouvez définir les tâches des clients et des groupes. Il existe deux types de tâches différentes : les tâches uniques et les tâches périodiques. Les tâches uniques sont exécutées à un moment défini. Pour les tâches périodiques, une planification est définie, en fonction de laquelle les tâches sont effectuées. Vous pouvez définir de nombreuses tâches différentes. Pour des raisons de performances, il est généralement plus raisonnable que les tâches ne se chevauchent pas, ni en temps ni en plage.

Dans la partie Tâches, les données suivantes sont listées pour toutes les tâches :

- **Nom** : vous pouvez saisir ici des noms longs et complets, qui détaillent précisément les tâches, de manière à conserver une vue d'ensemble des différentes tâches.
- **Type** : correspond au type de la tâche tel que tâche d'analyse ou tâche de détection de logiciel.
- **Client** : Les clients pour lesquels la/les tâches(s) ont été créée(s). Vous ne pouvez définir de tâches que pour les clients activés.
- **Groupe** : si vous créez une tâche de groupe, le nom du groupe (et non des clients) est affiché dans la liste d'ensemble.
- **Statut** : le statut ou le résultat des tâches. Vous pouvez ainsi déterminer si la tâche a déjà été effectuée, est terminée et si des virus ont été ou non détectés.
- **Dernière exécution** : cette colonne vous permet de déterminer quand la tâche a été effectuée pour la dernière fois.
- **Intervalle** : selon la planification que vous avez définie pour chaque tâche, ce champ indique la fréquence à laquelle la tâche est répétée.
- **Plage** : cette option indique les supports de données (disques durs locaux, par exemple) auxquels s'étend l'analyse.

Pour modifier une tâche, sélectionnez **Propriétés** depuis le menu contextuel (avec un clic droit).

Sinon, vous pouvez utiliser les options suivantes depuis la barre d'icônes située au-dessus de la liste de

tâches :

- **Rafraîchir**
- **Supprimer**
- **Tâche d'analyse unique** : cette fonction vous permet de définir des tâches d'analyse pour des clients ou des groupes de clients. Dans la boîte de dialogue de configuration, cliquez sur les onglets correspondants pour définir la plage, ainsi que d'autres paramètres d'analyse.
- **Tâche d'analyse périodique** : définit une tâche d'analyse périodique.
- **Tâche de sauvegarde** : Définit une tâche de sauvegarde pour des clients ou des groupes de clients (**module** Client Backup en option).
- **Tâche de restauration** : cette fonction permet de restaurer des sauvegardes centralisées sur des clients ou dans des groupes (**module** Client Backup en option).
- **Tâche de détection des logiciels** : cette fonction permet de détecter les logiciels installés sur les clients (**module** PatchManager en option).
- **Tâche de déploiement des logiciels** : Planifie le déploiement des logiciels et des correctifs (**module** PatchManager en option).
- **(Ré)exécuter immédiatement** : sélectionnez cette fonction pour exécuter de nouveau des tâches d'analyse uniques déjà effectuées ou interrompues. Si cette fonction est utilisée avec des tâches d'analyse périodiques, ces dernières sont alors exécutées immédiatement, indépendamment de la planification.
- **Journaux** : cette fonction vous permet d'ouvrir les journaux relatifs aux tâches du client concerné.
- **Afficher les tâches de groupe en détail** : affiche toutes les entrées relatives aux tâches de groupe. Cette option n'est disponible que lorsqu'un groupe est sélectionné dans la liste des ordinateurs.

Lorsque l'onglet Tâches est sélectionné, le menu **Tâches** apparait. Vous pouvez y effectuer les actions suivantes :

- **Afficher les tâches de groupe en détail**
- **(Ré)exécuter immédiatement** : vous pouvez directement exécuter les tâches sélectionnées, indépendamment des paramétrages planifiés.
- **Annuler** : cette fonction vous permet d'annuler la tâche en cours.
- **Supprimer** : cette fonction permet de supprimer les tâches sélectionnées.
- **Restaurer la sauvegarde** : cette option vous permet de lire les sauvegardes sur les clients via le réseau (option du **module de sauvegarde**).
- **Ajouter** : ce menu vous permet d'exécuter les actions susmentionnées.

4.3.10.1. Tâches d'analyse

La fenêtre **Nouvelle tâche d'analyse** permet aux administrateurs de définir des tâches d'analyse uniques ou récurrentes. Trois rubriques permettent de configurer ces tâches : **Planification des tâches**, paramètres du **Scanner** et **Plage d'analyse**. Ces trois rubriques sont accessibles par le biais d'un onglet spécifique.

Les options disponibles dépendent du type de clients pour lequel la tâche est planifiée : lorsqu'une tâche est planifiée pour un serveur Exchange par exemple (si Exchange Mail Security est installé), les

options spécifiques aux menaces de postes de travail ne sont pas disponibles.

Planification des tâches

L'onglet Tâches vous permet de planifier des tâches d'analyse.

- **Nom de la tâche** : Il est possible de définir ici le nom de la tâche d'analyse. Vous devez attribuer un nom évocateur comme *Analyse d'archives* ou *Analyse mensuelle* pour identifier facilement la tâche souhaitée et la retrouver dans le tableau synoptique.
- **Planification** (Analyse périodique) : Pour les tâches d'analyse régulières, vous pouvez indiquer quand et à quelle fréquence la vérification doit avoir lieu. Si vous sélectionnez **Au démarrage du système**, les directives de planification sont supprimées et le logiciel G DATA procède à la vérification au redémarrage de l'ordinateur. L'option **Tous les jours**, avec l'aide des indications sous **Jours de la semaine**, vous permet de définir si l'analyse antivirus n'est exécutée que durant les jours ouvrables, tous les deux jours ou le week-end, par exemple, quand l'ordinateur n'est pas utilisé à des fins professionnelles.
- **Heure** : Utilisez ce paramètre pour définir une heure de début. Une tâche d'analyse unique n'ayant pas d'heure de début, démarre immédiatement après la création de la tâche.
- **Paramètres**
  - **L'utilisateur peut interrompre ou annuler la tâche** : Des autorisations de suspension ou d'annulation de tâches peuvent être octroyées à l'utilisateur.
  - **Informer l'utilisateur en cas de détection de virus** : Affiche une notification sur l'écran, lorsqu'une menace est détectée.
  - **Envoi régulier de l'avancée de l'analyse au serveur (toutes les deux minutes)** : Cette option vous permet d'afficher le pourcentage de progression d'une tâche d'analyse en cours sur un client dans G DATA Administrator.
  - **Éteindre l'ordinateur après la vérification antivirus si aucun utilisateur n'est connecté** : La machine peut être automatiquement éteinte à la fin de l'analyse.
  - **Répéter la tâche si l'ordinateur n'est pas allumé à l'heure programmée** : Si l'ordinateur n'est pas allumé au moment défini pour la tâche d'analyse, cette option permet de lancer la tâche d'analyse lorsque l'ordinateur est démarré.
- **Contexte utilisateur (facultatif)** : Pour inclure l'analyse de partage réseau dans la tâche, il faut utiliser leurs chemins UNC plutôt que leurs lecteurs réseau mappés. Si la machine client n'a pas les droits d'accès (ex. *Client001$*) d'accès au partage, vous devez saisir ici les identifiants d'un compte ayant les droits appropriés.

Scanner

Les paramètres selon lesquels la tâche d'analyse doit être effectuée peuvent être définis dans le menu Scanner.

- **Utiliser les moteurs** : le logiciel G DATA fonctionne avec deux moteurs d'analyse antivirus fonctionnant indépendamment l'un de l'autre (voir **Paramètres du client** > **Outil de surveillance**).
- **En cas d'infection** : vous pouvez définir ici ce qui doit se passer lorsqu'un fichier infecté est détecté (voir **Paramètres du client** > **Outil de surveillance**).
- **Archives infectées** : indiquez ici comment les archives infectées doivent être traitées (voir **Paramètres du client** > **Outil de surveillance**).
- **Types de fichiers** : vous pouvez indiquer ici les types de fichiers dans lesquels des virus sont

recherchés. Notez qu'une vérification de tous les fichiers d'un ordinateur peut nécessiter un temps considérable.

- **Priorité du scanner** : les niveaux **Élevé**, **Intermédiaire** et **Faible** vous permettent de déterminer si G DATA doit accorder une haute priorité (l'analyse sera alors plus rapide, mais des baisses de performance sont possibles pour d'autres applications) ou une priorité faible (l'analyse sera alors plus longue, mais l'exécution des applications parallèles ne sera quasiment pas affectée) à l'analyse du système. Différents réglages sont ici possibles en fonction du moment de l'analyse.
- **Paramètres** : définissez les autres analyses antivirus que le logiciel G DATA doit effectuer. Les options choisies ici sont très utiles, mais, selon le type d'application, l'avantage du gain de temps lié à la suppression de ces vérifications peut générer une légère perte de sécurité. La plupart des paramètres sont identiques à ceux que vous pouvez définir au niveau de l'onglet **Paramètres du client** > **Outil de surveillance**. Des paramètres spécialement conçus pour les tâches d'analyse vous sont également proposés :
  - **S'assurer de l'absence de rootkit** : un rootkit essaie d'esquiver les méthodes de détection habituelles des virus. Vous pouvez, grâce à cette fonction, cibler votre recherche sur les rootkits sans effectuer une analyse complète des disques durs et des données enregistrées.
  - **Utiliser tous les processus** : si vous utilisez un système processeurs multi-cœurs, cette option vous permet de répartir les tâches du contrôle antivirus sur tous les processeurs. L'analyse antivirus peut ainsi s'effectuer beaucoup plus rapidement. L'inconvénient de cette option est que la puissance de calcul disponible pour les autres applications est moindre. Cette option ne doit être utilisée que si la tâche d'analyse doit être exécutée à des moments où le système n'est pas utilisé normalement (au cours de la nuit, par exemple).

Plage d'analyse

L'onglet Plage d'analyse permet de limiter l'analyse antivirus à certains répertoires (lorsqu'il s'agit d'un client) ou boites e-mail (lorsqu'il s'agit d'un serveur Exchange). La fenêtre de sélection du répertoire vous permet de sélectionner aussi bien des dossiers de l'ordinateur sur lequel G DATA Administrator est exécuté que des répertoires de clients sur lesquels fonctionne l'agent G DATA. Pour analyser des partages réseau, il faut utiliser leurs chemins UNC plutôt que leurs lecteurs réseau mappés. Vous pouvez aussi exclure des dossiers tels que ceux incluant des archives rarement utilisées. Une tâche d'analyse distincte sera alors créée pour les analyser.

4.3.10.2. Tâches de sauvegarde

La fonction de sauvegarde est un **module optionnel**.

Les administrateurs peuvent procéder ici à des tâches de sauvegarde des données des clients afin de sécuriser les fichiers importants de manière centralisée.

Planification des tâches

Il est possible de définir ici le **Nom de la tâche** de sauvegarde. Vous devez attribuer un nom évocateur comme *Sauvegarde mensuelle*ou *Sauvegarde partielle*du service extérieur pour identifier facilement la tâche souhaitée et la retrouver dans le tableau synoptique. Vous pouvez indiquer ici quand et à quelle fréquence les sauvegardes doivent être effectuées. Vous pouvez également indiquer s'il s'agit de Sauvegardes partielles ou de Sauvegardes complètes. Lors des sauvegardes partielles, seules les données modifiées depuis la dernière sauvegarde partielle ou complète sont enregistrées. Cela permet de gagner du temps lors de la création de la sauvegarde. La restauration des données est cependant plus longue étant donné que la dernière image du système doit être reconstituée à partir

des différents fichiers de données de sauvegardes partielles.

Pour éviter les problèmes liés à l'extinction d'un ordinateur portable non raccordé au réseau électrique, vous pouvez sélectionner le paramètre **Ne pas exécuter lors du fonctionnement sur batterie**. Les sauvegardes des périphériques mobiles ne sont alors effectuées que lorsque les périphériques sont raccordés au réseau électrique. L'option **Tous les jours**, avec l'aide des indications sous **Jours de la semaine**, vous permet de définir si l'analyse antivirus n'est exécutée que durant les jours ouvrables, tous les deux jours ou le week-end, par exemple, quand l'ordinateur n'est pas utilisé à des fins professionnelles.

Pour le serveur, le chemin vers le support de sauvegarde peut être configuré, tout comme les notifications, sous **Paramètres généraux** > **Sauvegarde**.

Sélection du fichier/répertoire
L'onglet **Sélection du fichier/répertoire** vous permet de sélectionner les données sauvegardées sur les différents clients/dans les différents groupes. Dans la rubrique **Portée de la sauvegarde**, vous pouvez sélectionner, dans l'arborescence des clients, les dossiers qui doivent être sauvegardés. La case **Exclure des fichiers** vous permet d'exclure de la sauvegarde des fichiers et des dossiers avec des attributs spécifiques (dossiers et fichiers temporaires, fichiers système, par exemple). Vous pouvez également définir des exceptions en ajoutant des extensions de fichiers à la liste des exceptions.

Si vous souhaitez enregistrer la sauvegarde créée dans un répertoire spécifique avant de la transférer au ManagementServer, vous pouvez l'indiquer explicitement sous **Mémoire cache**. Si l'option **Utiliser le chemin standard (en fonction du client)** n'est pas sélectionnée et qu'un chemin d'accès absolu est indiqué, la sauvegarde est enregistrée de manière temporaire dans le répertoire indiqué. Si vous sélectionnez cette option, l'application G DATA Security Client enregistre toujours la sauvegarde sur la partition disposant du plus d'espace mémoire disponible. Le répertoire G DATA\Backup est alors créé dans le répertoire racine de la partition.

4.3.10.3. Tâches de restauration

La fonction de restauration est un **module optionnel**.

Les tâches de restauration peuvent être planifiées de différentes manières. Dans le menu **Tâches**, cliquez sur **Nouveau** > **Tâche de restauration** ou sur le bouton **Tâche de restauration** dans la barre d'icônes. La fenêtre **Restaurer la sauvegarde** s'affiche et vous pouvez sélectionner la sauvegarde à restaurer. Vous pouvez également rechercher la sauvegarde dans la liste de tâches. Cliquez avec le bouton droit de la souris sur la tâche et sélectionnez **Restaurer la sauvegarde**.

La fenêtre Restaurer la sauvegarde affiche les informations de base concernant la tâche de sauvegarde sélectionnée. Elle inclut une ou plusieurs sauvegardes selon la fréquence à laquelle la tâche est exécutée. La liste affiche, pour chaque sauvegarde, l'**Heure de la sauvegarde**, le **Client**, le **Type de sauvegarde**, le **Nombre de fichiers** et la **Taille (en Mo)**. Dans la liste **Restaurer sur le client**, vous pouvez sélectionner le client sur lequel les fichiers doivent être restaurés (cela ne doit pas nécessairement être le client sur lequel la sauvegarde a été créée). Cliquez sur **OK** pour ouvrir la fenêtre des paramètres de restauration.

Deux onglets permettent de configurer les paramètres de restauration. L'option **Sélection de fichiers** vous permet de rechercher la sauvegarde. Cliquez sur **Restaurer uniquement les fichiers sélectionnés de l'archive**, pour sélectionner une structure de dossiers dont les fichiers doivent être restaurés. Cliquez sur **Restaurer tous les fichiers de l'archive** pour désactiver la structure de dossiers et restaurer tous les fichiers. L'onglet **Options** vous permet de configurer les paramètres des

tâches. Sous **Nom de la tâche**, saisissez un nom évocateur. Si vous souhaitez rétablir les fichiers dans les répertoires d'origine, activez l'option **Rétablir les fichiers dans les répertoires d'origine**. Vous pouvez également sélectionner un **Répertoire cible différent**. Pour terminer, vous pouvez déterminer ce qui doit se passer en cas de conflit de version avec les fichiers existants. Après confirmation des paramètres, la tâche de restauration est ajoutée au module des tâches et immédiatement exécutée.

4.3.10.4. Tâches de détection des logiciels

Le module PatchManager est un **module optionnel**.

La tâche de recherche des correctifs peut être planifiée pour vérifier si un ou plusieurs correctifs sont applicables sur les clients ou les groupes. Les tâches peuvent être planifiées selon les options suivantes :

- **Exécution** : décide quand la tâche d'application du correctif doit être exécutée :
  - **Synchronisé** : Exécute la tâche d'application du correctif selon une **Planification**, qui est définie selon les paramètres suivants : **Immédiatement**, **Une fois**, **Toutes les heures**, **Tous les jours**, **Toutes les semaines**, **Tous les mois** ou **Lors de la connexion Internet**.
  - **Dès que disponible** : Exécute la tâche d'application du correctif chaque fois qu'un correctif est disponible.

Pour sélectionner les patches pour lesquels la tâche d'application doit être vérifiée, utilisez une des deux options de **Plage** suivantes :

- **Patch spécifique** : sélectionnez un ou plusieurs correctifs dans la liste.
- **Propriété** : Utiliser une **Propriété** pour sélectionner un éventail de patches en utilisant un mot-clé. Pour ajouter une propriété spécifique (**Fabricant**, **Nom de produit**, **Urgence**, Langue) comme critère pour filtrer, cochez la case et entrez un mot-clé. Ainsi vous pouvez vérifier l'application pour les patches d'un éditeur spécifique ou seulement pour des versions spécifiques. Des signes tels que *?*et *** peuvent être utilisés. Activez l'option **Correctifs uniquement** si la tâche ne doit pas être exécutée pour l'application de logiciels entiers ou pour des mises à niveau.

Sélectionnez **Installer automatiquement les patches applicables** pour être sûr que chaque fois qu'un patch applicable est trouvé, il sera automatiquement installé.

Si la tâche d'application des correctifs a été planifiée directement à partir de la **Vue d'ensemble des statuts** de PatchManager, la tâche s'applique aux correctifs et clients sélectionnés ici. Si elle a été planifiée à partir du module **Configuration des correctifs**, il faut sélectionner les clients pour lesquels l'applicabilité sera vérifiée. Si elle a été planifiée à partir du module **Tâches**, il faut sélectionner les correctifs qui doivent être vérifiés – la tâche s'appliquera aux groupes ou aux clients utilisés dernièrement.

4.3.10.5. Tâches de déploiement des logiciels

Le module PatchManager est un **module optionnel**.

Pour déployer les **correctifs applicables** aux clients ou aux groupes, vous pouvez définir une tâche de déploiement des logiciels.

Les tâches de déploiement des logiciels peuvent être administrées et planifiées grâce à l'option **Planification** :

- **Immédiatement** : La tâche de déploiement des logiciels s'exécute immédiatement.
- **Directement après l'amorçage** : La tâche de déploiement des logiciels s'exécutera après le prochain amorçage.
- **Directement après la connexion** : La tâche de déploiement des logiciels s'exécutera après la prochaine connexion de l'utilisateur au client.
- **Exécuter à une heure** : Planifie la tâche afin qu'elle s'exécute après une heure définie (l'autre option de planification ne sera pas effective jusqu'à l'heure définie).
- **Différer la tâche** : Planifier un délai pour démarrer la tâche. Ainsi, le processus d'amorçage et la tâche de déploiement n'influencera pas les performances du client.

Si la tâche de distribution des logiciels a été planifiée à partir de la **Vue d'ensemble des statuts** de PatchManager, la tâche s'applique aux correctifs et clients sélectionnés. Si elle a été planifiée depuis le module **Configuration des correctifs**, vous devez sélectionner le(s) client(s) pour qui le patch doit être installé. Si elle a été planifiée depuis le module **Tâches**, vous devez sélectionner les patchs à installer – ils seront installés sur le groupe ou le client sélectionné précédemment.

4.3.10.6. Tâches de retour en arrière

Le module PatchManager est un **module optionnel**.

Pour désinstaller des correctifs déjà installés, vous devez procéder à un retour en arrière via le module **PatchManager**. Vous pouvez également cliquer avec le bouton droit de la souris sur la tâche de distribution correspondante dans la liste des tâches et sélectionner la fonction **Retour en arrière**.

La fenêtre de **Retour en arrière des mises à jour** vous demande d'indiquer un **Nom de tâche** pour identifier plus facilement les tâches de retour en arrière. Après avoir indiqué un nom, cliquez sur **OK** pour ajouter une tâche à la liste des **Tâches**. L'exécution sera immédiate.

4.3.11. PolicyManager

Le module PolicyManager est uniquement disponible dans les **versions logicielles** Endpoint Protection Business et Managed Endpoint Security.

Le module PolicyManager permet de contrôler les applications, les périphériques et les contenus Internet et de surveiller le temps d'utilisation d'Internet. Ces fonctions permettent une mise en œuvre intégrale des directives de l'entreprise pour l'utilisation des PC de l'entreprise. PolicyManager permet ainsi de définir si, et dans quelle mesure, des supports de stockage de masse ou optiques peuvent être utilisés. Il est également possible de définir les sites Web visités et les programmes qui peuvent être utilisés sur les PC de l'entreprise.

4.3.11.1. Contrôle des applications

Le contrôle des applications vous permet de bloquer l'utilisation de certains programmes sur les clients sélectionnés. Pour ce faire, indiquez sous **Statut** si les limitations s'appliquent à tous les utilisateurs du client ou uniquement aux utilisateurs qui ne disposent pas d'autorisations d'administrateur au niveau de l'ordinateur client. Sous **Mode**, indiquez si la liste de contrôle des applications est une liste blanche ou une liste noire.

- **Liste blanche** : seules les applications indiquées ici peuvent être utilisées par l'ordinateur client.
- **Liste noire** : les applications indiquées ici ne peuvent pas être utilisées par l'ordinateur client.

Via le bouton **Nouveau**, vous pouvez créer une nouvelle règle. Les types de règles Fabricant, Fichier et Répertoire sont disponibles.

- **Fabricant** : les informations relatives au créateur du programme sont utilisées pour autoriser ou interdire l'utilisation des applications. Vous pouvez saisir le nom du fabricant ou utiliser l'option ... pour sélectionner de manière ciblée un fichier à partir duquel les informations du fabricant sont lues et appliquées.
- **Fichier** : vous pouvez bloquer ou autoriser certains fichiers du programme pour le client. Vous pouvez saisir les noms des fichiers pour lesquels vous souhaitez interdire ou autoriser l'accès de manière générale. Vous pouvez également cliquer sur le bouton **Déterminer les caractéristiques** d'un fichier pour sélectionner un fichier en fonction de ses caractéristiques. Si nécessaire, vous pouvez utiliser un astérisque (*) au début et/ou à la fin de la caractéristique **Nom du fichier**, **Nom du produit** ou **Droits d'auteur**.
- **Répertoire** : cette fonction vous permet d'autoriser ou de bloquer des répertoires entiers (sous-répertoires inclus, si vous le souhaitez) pour les clients.

4.3.11.2. Contrôle des périphériques

Le contrôle des périphériques permet de limiter l'accès aux périphériques et supports mémoire externes. Vous pouvez ainsi interdire l'utilisation de supports de stockage (clés USB, disque dur, téléphone), attribuer des droits en écriture ou en lecture aux lecteurs de CD/DVD ou limiter l'utilisation des caméras.

Sous **Statut** indiquez si les restrictions s'appliquent à tous les utilisateurs du client ou uniquement aux utilisateurs qui ne disposent pas de droits d'administrateur au niveau de l'ordinateur client.

Dans la section Périphériques vous pouvez définir les autorisations pour chaque type de périphérique :

- **Permissions** :
  - **Lire/écrire** : l'accès au périphérique est illimité.
  - **Lire** : les supports peuvent uniquement être lus, il est interdit d'enregistrer des données.
  - **Interdire l'accès** : l'accès, en lecture ou en écriture, au périphérique est interdit. Le périphérique ne peut pas être utilisé par l'utilisateur.
- **Permission temporaire** : Lorsqu'une permission temporaire a été accordée via une demande de déblocage dans le PolicyManager, la période de grâce accordée est indiquée ici. Cliquez sur le symbole X pour annuler la période de grâce.

En configurant les Exceptions, vous pouvez de nouveau autoriser l'utilisation des périphériques dont vous aviez restreint l'emploi (Lire/Interdire l'accès). Cliquez sur Ajouter pour ouvrir une boîte de dialogue dans vous pouvez définir des exceptions.

- **Périphérique** : Sélectionnez le type de périphérique pour lequel vous souhaitez ajouter une exception.
- **Règle active** : L'exception n'est valable que si la case correspondante est cochée
- **Type** :
  - **Exception en fonction du type de périphérique** : Ici c'est le type de **Périphérique** qui est utilisé pour mettre en place l'exception.
  - **Exception en fonction de l'identifiant du matériel/du support** : ici c'est l'identifiant d'un **Périphérique** ou d'un support qui est utilisé pour mettre en exception un périphérique

ou support spécifique (exemple une clé USB ou un DVD)

- **Autorisation** : Choisissez le type d'accès que vous souhaitez autoriser.
- **Identifiant du matériel/Identifiant du support** : Lorsque vous avez choisi **Exception en fonction de l'identifiant du matériel/du support**, saisissez identifiant matériel correspondant . Cliquez sur le bouton **...** pour récupérer l'identifiant d'un matériel ou d'un support.
  - **Sélectionner la source** : Choisir **(recherche locale...)** afin de récupérer l'identifiant d'un matériel ou un support qui se trouve sur la machine sur laquelle est lancé G DATA Administrator. Pour déterminer l'identifiant d'un matériel ou un médium se trouvant sur une autre machine, sélectionnez là depuis la liste de machine disponible.
  - **Périphérique** : Choisir **Utiliser l'identifiant du support** pour afficher l'identifiant du support (ex. CD/DVD) ou **Utiliser l'identifiant du matériel** pour afficher l'identifiant du matériel.
- **Définir l'utilisateur/le groupe Windows** : Si l'exception doit s'appliquer à des utilisateurs ou des groupes Windows, veuillez les insérer ici. Pour saisir plusieurs utilisateurs/groupes, veuillez les séparer par une virgule « , » ou un retour à la ligne.
- **Commentaire** : Ajoutez un commentaire explicatif pour pouvoir distinguer et identifier les différentes règles.

4.3.11.3. Contrôle du contenu Web

Le contrôle du contenu Web vous permet d'autoriser les utilisateurs à accéder à Internet à des fins professionnelles et d'interdire la consultation de sites Web non désirés et relevant de certains thèmes. Vous pouvez autoriser ou refuser des rubriques ciblées en cochant ou en décochant les cases des clients. Les catégories couvrent une grande quantité de domaines thématiques et sont actualisées en permanence par G DATA. L'administrateur réseau n'a donc plus à gérer les listes blanches et noires.

Sous **Statut** indiquez si les restrictions s'appliquent à tous les utilisateurs du client ou uniquement aux utilisateurs qui ne disposent pas de droits d'administrateur au niveau de l'ordinateur client.

Grâce à la section **Exceptions globale**, vous pouvez, indépendamment des paramètres définis sous **Catégories autorisées**, autoriser ou bloquer certains sites Internet pour l'ensemble du réseau, à l'échelle de l'entreprise. Cette action s'effectue en cliquant sur **Ajouter**, suivi de la sélection de l'action à faire (**Autoriser** ou **Verrouiller**) puis de la saisi de l'adresse (sans information sur le protocole) du site à mettre en exception et enfin en cliquant sur **OK** pour valider. Les boutons **Modifier** et **Supprimer** permet de faire les actions indiquées par leur nom.

4.3.11.4. Temps d'utilisation d'Internet

Dans la zone Temps d'utilisation d'Internet, l'utilisation générale d'Internet peut être limitée à des durées définies. La définition d'un quota de temps pour l'utilisation d'Internet est possible. Sous **Statut**, indiquez si les restrictions s'appliquent à tous les utilisateurs du client ou uniquement aux utilisateurs qui ne disposent pas de droits d'administrateur au niveau de l'ordinateur client. Le curseur de la page de droite permet de définir le quota mis à disposition sur chaque ordinateur client pour l'utilisation d'Internet. Des quotas journaliers, hebdomadaires ou mensuels peuvent être attribués : l'indication *04 20:05* correspond à une durée d'utilisation d'Internet de 4 jours, 20 heures et 5 minutes, par exemple.

> C'est toujours la plus petite valeur qui compte dans l'interaction des quotas d'utilisation Internet. Par exemple, si vous définissez une limite d'utilisation de quatre jours dans le mois

mais autorisez cinq jours dans la semaine, le logiciel réglera automatiquement l'utilisation d'Internet de l'utilisateur sur quatre jours.

Si un utilisateur essaie d'accéder à Internet alors que son quota d'accès est dépassé, le navigateur affiche une fenêtre l'avertissant du dépassement de quota. En plus de la limitation de durée (partie droite), vous pouvez aussi restreindre l'utilisation d'internet suivant des plages horaires (partie gauche). Les périodes bloquées sont représentées en rouge et les périodes autorisées en vert. Pour autoriser ou bloquer une période, il vous suffit de la sélectionner avec la souris. Avec le clic droit, le menu contextuel s'affiche et vous offre deux possibilités : **Débloquer du temps** et **Bloquer du temps**. Lorsqu'un utilisateur essaie d'accéder à Internet durant une période bloquée, le navigateur affiche un écran l'avertissant que l'accès à Internet n'est pas autorisé à ce moment-là.

4.3.12. Pare-feu

Le module Pare-feu est disponible comme partie des **solutions** Client Security Business, Endpoint Protection Business et Managed Endpoint Security.

4.3.12.1. Vue d'ensemble

Cette rubrique permet d'administrer de manière centralisée le module Pare-feu sur des clients ou dans des groupes.

Paramètres
Vous pouvez définir ici quelques paramètres généraux du pare-feu :

- **Activer G DATA Firewall**: Active/désactive le pare-feu

  Note : A partir de la version 14, les clients sur lesquels le pare-feu n'est pas installé, doivent être mis à niveau vers la nouvelle version avant que le pare-feu ne puisse être activé.
- **Signaler les applications bloquées** : lorsque cette case est cochée et que l'ordinateur client peut se connecter à G DATA ManagementServer, l'administrateur système reçoit, dans la rubrique **Événements de sécurité** des informations sur les applications bloquées par le pare-feu client en question.
- **Jeu de règle**: Permet de choisir le jeu de règle à utiliser
  - **Mode pilote automatique**: Les règles sont configuré automatiquement par G DATA. Le pare-feu effectue sa mission en arrière-plan sans déranger l'utilisateur. En mode Pilote automatique le pare-feu optimise les règles.
  - Un des jeux de règles créés par l'administrateur.

Fonctionnement au sein du réseau interne
Configurez le champ d'action qui est autorisé à l'utilisateur lorsqu'il est au sein du réseau où se trouve son ManagementServer.

- **L'utilisateur peut activer/désactiver le pare-feu** : en tant qu'administrateur réseau, vous pouvez permettre à l'utilisateur de l'ordinateur client de désactiver le pare-feu. Cette possibilité n'est accordée que si le client se trouve au sein du réseau d'entreprise et elle devrait être réservée aux utilisateurs initiés.

Fonctionnement hors du réseau interne
Configure le champ d'action qui est autorisé à l'utilisateur lorsqu'il est en dehors du réseau où se trouve son ManagementServer.

- **Utiliser la configuration hors site pour les clients mobiles** : pour une plus grande flexibilité

dans la protection des ordinateurs portables, une règle hors-site peut être automatiquement appliquée lorsque les ordinateurs sont en dehors du réseau de leur ManagementServer. Aussitôt que l'ordinateur retourne dans son réseau d'origine, le jeu de règles habituel est de nouveau appliqué.

Note : La configuration hors site peut uniquement être utilisée lorsque le pare-feu du réseau de l'entreprise ne fonctionne pas en mode de pilote automatique.

- **Jeu de règle**: Sélectionnez le jeu de règles qui devrait être utilisé par le client hors-site.
  - **Mode pilote automatique** (voir **Pare-feu** > **Vue d'ensemble** > **Paramètres**).
  - Un des jeux de règles créés par l'administrateur.
- **L'utilisateur peut modifier la configuration hors site** : cette option permet aux utilisateurs expérimentés de configurer leur pare-feu individuellement lorsqu'ils sont hors du réseau. Dès que l'ordinateur portable est de nouveau connecté à son réseau d'origine, les modifications effectuées sont remplacées par les règles définies par l'administrateur.

4.3.12.2. Ensembles de règles

L'onglet Ensembles de règles vous permet de créer des ensembles de règles pour différents réseaux. Chaque ensemble de règles peut avoir un nombre indéfini de règles.

Le jeu de règles. Les jeux de règles se gère via les boutons **Nouveau**, **Supprimer**, **Importer** et **Exporter**. Les paramètres suivants se configurent dans la section paramètres :

- **Nom** : Nom du jeu de règles sélectionné.
- **Commentaire** : Description du jeu de règles sélectionné.
- **Mode furtif actif** : Bloque les demandes d'ordinateurs qui tentent de tester les ports ouverts. Complique la tâche aux attaquants voulant collecter des informations sur le système.

Les règles du jeu de règles sélectionné sont listées dans la partie basse de l'onglet.

Dans la section Règles vous pouvez **créer, modifier**, supprimer une règle ou lancer l'**assistant**. Les règles sont exécutées dans leur ordre de classement. La section **Classement** vous permet de réarranger les règles à votre convenance grâce aux boutons **Début**, **Haut**, **Bas** et **Fin**.

Créer un ensemble de règles

Sélectionnez **Ensembles de règles** et cliquez sur **Nouveau** pour ouvrir une nouvelle fenêtre. Entrez un nom pour l'ensemble de règles et une note ou un commentaire optionnel. Sélectionner le mode furtif bloque les requêtes adressées à l'ordinateur visant à contrôler l'accessibilité d'un port. Il est ainsi plus difficile pour les auteurs d'attaques de recueillir des informations sur le système.

Dans la section **Sélectionnez ici les règles de l'ensemble par défaut que vous souhaitez utiliser**, cochez/décochez les cases en fonction des règles que vous souhaitez utiliser. Une fois validé, le jeu de règle est disponible dans la liste de jeu de règles.

Créer une règle/Modifier une règle

Sous **Règles**, utilisez les boutons **Nouveau** et **Modifier** pour ajouter de nouvelles règles ou modifier des règles existantes.

- **Nom** : c'est le nom du programme auquel s'applique la règle pour les règles prédéfinies et générées automatiquement.
- **Règle active** : Active/désactive la règle sans la supprimer.

- **Commentaire** : indique la manière dont la règle a été créée. Pour les règles prédéfinies pour l'ensemble de règles, l'option est la suivante : *Règle prédéfinie*. L'option *Générée après l'avertissement* est destinée aux règles créées dans la boîte de dialogue de l'alerte du pare-feu. Pour les règles que vous créez par l'intermédiaire de la boîte de dialogue destinée aux personnes averties, vous pouvez ajouter vos propres commentaires.
- **Sens de connexion** : le sens détermine si la règle s'applique aux connexions entrantes, sortantes ou aux deux.
- **Accès** : indique si l'accès doit être autorisé ou refusé pour le programme concerné par cet ensemble de règles.
- **Protocole** : vous pouvez choisir les protocoles de connexion pour lesquels vous autorisez ou refusez l'accès. Il est possible de bloquer ou d'autoriser les protocoles de façon permanente ou de coupler l'utilisation du protocole à l'utilisation d'une ou de plusieurs applications en particulier (**Lier à une/des application(s)**). Vous pouvez de la même manière définir les ports autorisés ou interdits à l'aide du bouton **Attribuer le service Internet**.
- **Période** : vous pouvez également définir une plage horaire pendant laquelle l'accès aux ressources réseau est autorisé (n'autoriser l'accès que pendant vos heures de travail et l'interdire en dehors de celles-ci, par exemple).
- **Plage d'adresses IP** : pour les réseaux avec adresses IP fixes, il est utile de réglementer leur utilisation en limitant la plage d'adresses IP autorisée. Une plage d'adresses IP clairement définie réduit nettement le risque d'intrusion.

Assistant de règles

L'assistant de règles vous permet d'ajouter ou modifier des règles d'un ensemble de règles.

L'assistant de règles vous propose les actions suivantes :

- **Autoriser ou refuser l'accès à une application** : vous pouvez sélectionner de manière ciblée une application et lui autoriser ou lui interdire l'accès au réseau dans le cadre de l'ensemble de règles choisi. Pour cela, il vous suffit de sélectionner dans l'assistant le programme de votre choix (chemin d'accès au programme) et d'indiquer sous **Sens de connexion** s'il doit être bloqué pour les connexions entrantes, pour les connexions sortantes ou pour les connexions entrantes et sortantes. Vous pouvez ainsi interdire à votre lecteur MP3 de transmettre des données sur vos habitudes d'écoute (connexions sortantes) ou empêcher les mises à jour automatiques du programme (connexions entrantes).
- **Ouvrir ou bloquer un service Internet (port) défini** : l'assistant vous permet de bloquer les ports de votre choix, entièrement ou uniquement pour une application définie (logiciel de gestion des relations avec la clientèle, par exemple).
- **Ajouter une ou plusieurs règles par défaut** : ajoute la règle depuis l'ensemble de règles par défaut à l'ensemble de règles sélectionné.
- **Copier une règle existante** : cette fonction vous permet de copier une règle existante de manière à la modifier.

4.3.13. PatchManager

Le module PatchManager est un **module optionnel**.

PatchManager vous permet de gérer, via une seule interface, la mise en application des correctifs pour tous les clients administrés. Vous pouvez utiliser PatchManager pour administrer les mises à jour

des logiciels Microsoft, mais également des logiciels d'autres éditeurs. Vous pouvez vérifier que chaque correctif peut bien être utilisé, bloquer les correctifs, les distribuer ou annuler leur installation par un retour en arrière. Le module peut être utilisé sur les clients ou les groupes de clients.

4.3.13.1. Vue d'ensemble des statuts

La rubrique Vue d'ensemble des statuts vous offre une vue d'ensemble détaillée des correctifs et de leur statut au sein du réseau. La rubrique répertorie tous les correctifs disponibles par ordre alphabétique et une fois par client. Il est possible de filtrer cette liste complète pour déterminer si tous les clients ont été mis à jour avec tous les correctifs pertinents, par exemple. Vous pouvez également programmer la mise à disposition des correctifs. Un ensemble de graphiques vous montre les informations sur les correctifs en suspens et peut être utilisé pour visualiser rapidement si des correctifs importants doivent être installés.

Cette vue d'ensemble est regroupée par défaut en fonction du **Statut**, de la **Priorité**, du **Fabricant** et du **Produit** pour définir rapidement si les correctifs essentiels sont déjà installés ou non. La configuration par défaut du filtre de l'affichage exclut les installations de logiciels complet, tout comme les entrées bloquées. Cliquez sur **Réinitialiser tous les filtres** pour réinitialiser les filtres. L'affichage des correctifs qui remplacent un correctif précédent peuvent être étendus ; cliquez sur le signe plus pour afficher tous les patchs remplacés.

Selon le correctif et le client, différents types de tâches de corrections peuvent être planifiées. Cliquez-droit sur un ou plusieurs correctifs et sélectionnez une des options suivantes :

- **Vérifier que les correctifs peuvent être appliqués** : Planifier une tâche qui vérifie si les patchs sélectionnés sont applicables aux clients sélectionnés, avec la fenêtre **Détection du logiciel**.
- **Installer les correctifs** : Planifier une tâche qui installe un ou plusieurs correctifs sur les clients sélectionnés par la fenêtre **Déploiement du logiciel**.
- **Retour en arrière** : Planifier une tâche de retour en arrière pour des correctifs qui ont déjà été déployés sur les clients sélectionnés en utilisant la fenêtre de **Retour en arrière**.
- **Empêcher l'installation de correctifs** : Bloque le déploiement d'un ou plusieurs correctifs qui ne doivent pas être distribués aux clients. Les correctifs bloqués seront ignorés lors de l'exécution automatique des tâches de détection et de déploiement. Lors de la planification manuelle d'une tâche d'applicabilité ou de déploiement, les correctifs bloqués sont cachés par défaut.
- **Débloquer l'installation de correctifs** : Débloque un ou plusieurs correctifs.
- **Propriétés** : Plus d'informations, incluant une description complète et la licence.

La colonne **Statut** affiche le statut de tous les correctifs (par exemple : *Contrôle en cours* quand la tâche est en train de s'exécuter ou *Non applicable* quand le correctif ne peut être appliqué).

4.3.13.2. Paramètres

Vous pouvez indiquer comment les correctifs et les mises à jour sont accessibles pour les clients et dans les groupes.

- **Activer la gestion des correctifs** : activer ou désactiver PatchManager.
- **Mode** : décide si PatchManager doit exécuter automatiquement les tâches de d'applicabilité et d'installation :
  - **Manuel** : PatchManager n'exécutera pas automatiquement les tâches d'applicabilité et

d'installation

- **Vérifier l'applicabilité des correctifs prioritaires** : quand un correctif avec une priorité haute est disponible, PatchManager exécutera automatiquement les tâches de déploiement sur tous les clients. Cela évite de planifier des tâches de déploiement.
- **Installer les correctifs prioritaires automatiquement** : quand un correctif avec une priorité importante est disponible, PatchManager l'installera automatiquement (exécutera automatiquement une tâche de déploiement sur tous les clients si le patch est applicable). Cela pouvant générer des problèmes de compatibilité, il est recommandé de vérifier les correctifs sur un certain nombre de clients test avant de le déployer sur les clients.

- **L'utilisateur peut afficher et demander des correctifs** : sélectionnez cette option pour qu'un utilisateur puisse afficher les correctifs disponibles et soumettre une requête pour le déploiement.
- **L'utilisateur peut refuser l'installation des correctifs** : sélectionnez cette option pour donner à l'utilisateur la possibilité de refuser l'installation d'un correctif, au moins temporairement. Vous pouvez indiquer la fréquence avec laquelle l'utilisateur peut refuser l'installation jusqu'à ce que celle-ci soit exécutée de force ainsi que la fréquence des tentatives d'installation de correctifs par le système.

4.3.13.3. Configuration des correctifs

La rubrique Configuration des correctifs vous permet de gérer de manière centralisée tous les correctifs connus à l'échelle du système. Un ensemble de graphiques vous montre des statistiques sur les correctifs, les produits et les fabricants.

Les correctifs sont regroupés par défaut par **Fabricant**, **Produit** et **Priorité** afin de vous permettre de retrouver rapidement les correctifs pour le produit correspondant. La configuration par défaut du filtre de l'affichage exclut les installations de logiciels complet, tout comme les entrées bloquées. Cliquez sur **Réinitialiser tous les filtres** pour réinitialiser les filtres. L'affichage des correctifs qui remplacent un correctif précédent peuvent être étendus ; cliquez sur le signe plus pour afficher tous les patchs remplacés.

Selon les patchs, différents types de tâches de corrections peuvent être appliqués. Un clic droit sur un ou plusieurs correctifs vous donne accès aux options suivantes :

- **Vérifier que les correctifs peuvent être appliqués** : Planifier une tâche qui vérifie si les patchs sélectionnés sont applicables aux clients sélectionnés, avec la fenêtre **Détection du logiciel**.
- **Installer les correctifs** : Planifier une tâche qui installe un ou plusieurs correctifs sur les clients sélectionnés par la fenêtre **Déploiement du logiciel**.
- **Empêcher l'installation de correctifs** : Bloque le déploiement d'un ou plusieurs correctifs qui ne doivent pas être distribués aux clients. Les correctifs bloqués seront ignorés lors de l'exécution automatique des tâches de détection et de déploiement. Lors de la planification manuelle d'une tâche d'applicabilité ou de déploiement, les correctifs bloqués sont cachés par défaut.
- **Débloquer l'installation de correctifs** : Débloque un ou plusieurs correctifs.
- **Propriétés** : Plus d'informations, incluant une description complète et la licence.

La colonne **Priorité** affiche la priorité de chaque correctif. Vous pouvez également modifier la priorité indiquée ici, qui est basée sur les informations de la base de données interne du PatchManager.

4.3.14. Protocoles

L'onglet Protocoles liste les **Évènements de sécurité** client tels que la découverte de virus ou les demandes de déblocage PolicyManager et **Journaux d'infrastructure** tel que les changements de configuration ou le statut de tâches d'analyse.

4.3.14.1. Événements de sécurité

Toutes les notifications du logiciel G DATA sont affichées dans le module Événements de sécurité. Parmi elles, on compte les virus détectés, les messages de l'application PolicyManager, les rapports PatchManager ou du pare-feu, mais aussi les messages du système au sujet des installations. Le statut de l'évènement est affiché dans la colonne des **Statut** (par exemple : **Virus trouvé** ou **Fichier déplacé en quarantaine**).

Si vous avez configuré les tâches d'analyse pour uniquement journaliser les attaques de virus, vous pouvez intervenir sur elles en sélectionnant une ou plusieurs entrées de la liste, puis une commande à partir du menu contextuel (clic droit de la souris), du menu **Événements de sécurité** ou de la barre d'icônes. Vous pouvez supprimer ou mettre en quarantaine les fichiers infectés.

Le menu **Évènements de sécurité** et le menu contextuel (clic droit) proposent les fonctions suivantes :

- **Affichage** : Choisissez comment va s'afficher la liste d'évènements :
  - **Masquer les rapports dépendants** : Permet de cacher les rapports identiques et de n'afficher que le plus récents d'entre eux (se base sur les champs **Clients**, **Expéditeur** et **Fichier/courrier/contenu**).
  - **Masquer les rapports lus** : Cache les rapports déjà lus.
- **Supprimer le virus du fichier** (pour les rapports d'analyse de virus uniquement) : le système tente de supprimer les virus du fichier d'origine.
- **Mettre le fichier en quarantaine** (pour les rapports d'analyse de virus uniquement) : cette fonction déplace les fichiers sélectionnés dans le dossier de quarantaine. Les fichiers sont chiffrés et enregistrés dans le dossier de quarantaine de G DATA ManagementServer. Les fichiers d'origine sont effacés. Le chiffrement vous garantit que le virus n'est plus en mesure de provoquer des dommages. Sachez que chaque fichier mis en quarantaine dispose d'un rapport. Si vous supprimez le rapport, le fichier du dossier de quarantaine est également effacé. Vous pouvez envoyer un fichier du dossier de quarantaine au service antivirus d'urgence afin qu'il y soit analysé. Ouvrez pour cela le menu contextuel d'un rapport de quarantaine d'un clic droit. Une fois le motif de l'envoi sélectionné, cliquez sur le bouton **OK** de la boîte de dialogue du rapport.
- **Supprimer le fichier** (pour les rapports d'analyse de virus uniquement) : le fichier d'origine est supprimé au niveau du client.
- **Définir en tant qu'exception du Gardien** (seulement pour les rapports du Gardien via la menu contextuel) : Ajoute une exception pour le Gardien (**Paramètres du client** > **Gardien** > **Paramètres**).
- **Définir les exceptions pour la protection anti-exploit** (seulement pour les rapports de ExploitProtection via le menu contextuel): Ajoute une exception à la liste blanche de ExploitProtection (**Paramètres** > **Gardien** > **ExploitProtection**).
- **Annuler l'autorisation du clavier**: supprime l'autorisation USB Keyboard Guard donné précédemment par l'utilisateur.

- **Quarantaine : désinfecter puis restaurer le fichier** (uniquement pour les rapports de virus en quarantaine) : le système tente de supprimer le virus du fichier. En cas de suppression réussie, le fichier nettoyé est renvoyé vers son emplacement d'origine sur le client. Si le virus ne peut être supprimé, le fichier n'est pas réinséré.
- **Quarantaine : restaurer** (uniquement pour les rapports de virus en quarantaine) : cette option permet de déplacer un fichier du dossier de la quarantaine vers le client. **Attention** : le fichier est replacé dans son état d'origine et est donc toujours infecté.
- **Quarantaine : envoyer au service G DATA Security Labs** (uniquement pour les rapports de virus en quarantaine) : en cas de nouveau virus ou de phénomène inconnu, faites-nous parvenir le fichier à l'aide de la fonction Quarantaine du logiciel G DATA. Nous traitons bien sûr toutes les données envoyées avec confidentialité et discrétion.
- **Quarantaine : supprimer le fichier et le rapport** (uniquement pour les rapports de virus en quarantaine) : les rapports sélectionnés sont supprimés. Si un fichier de quarantaine est lié aux rapports à supprimer, la suppression doit être confirmée une nouvelle fois. Les fichiers se trouvant en quarantaine sont alors également supprimés.
- **Ajouter l'adresse URL à la liste blanche** (uniquement pour les rapports **Contrôle du contenu Web**) : Ajouter l'URL correspondante à la liste blanche générale.
- **Ajouter l'adresse URL à la liste noire** (uniquement pour les rapports **Contrôle du contenu Web**) : Ajouter l'URL correspondante à la liste noire générale.
- **Supprimer le rapport** : cette fonction vous permet de supprimer les rapports sélectionnés. Si un fichier de quarantaine est lié aux rapports à supprimer, la suppression doit être confirmée une nouvelle fois. Les fichiers se trouvant en quarantaine sont alors également supprimés.
- **Nettoyer les rapports** : Supprime les duplicatas de rapports en gardant le plus récent.

  La commande Nettoyer les rapports ne nettoie que les rapports affichés dans la page active. Si des filtres masquent des rapports ou si les rapports se trouvent sur une autre page que celle affichée à l'écran, ils ne seront pas affectés par la commande de nettoyage.
- **Exporter les rapports** (Seulement via le menu contextuel): export le(s) rapport(s) sélectionné(s) ou la liste entière en tant que fichier XML.
- **Marquer comme lu** (Seulement via le menu contextuel): marque le(s) rapport(s) sélectionné(s) comme lu.
- **Marquer comme non lu** (Seulement via le menu contextuel): marque le(s) rapport(s) sélectionné(s) comme non lu.
- **Détails/Actions** (Seulement via le menu contextuel): Certains évènements vous permettent directement de planifier une tâche. Par exemple, si un client a demandé un retour en arrière (rollback), vous pouvez faire un clic droit sur cette demande et sélectionnez **Détails/Actions**. Dans la fenêtre **Répartir le logiciel (retour en arrière)**, vous pouvez directement planifier une tâche de retour en arrière sans ouvrir le module **PatchManager** pour sélectionner le correctif et le client.

La barre d'icônes du module Évènements de sécurité propose les options et de paramètres de filtrage suivants :

 **Rafraîchir**

 **Supprimer**

 **Imprimer**

 **Affichage des pages**

- **Supprimer le virus**
- **Mettre en quarantaine**
- **Supprimer le fichier**
- **Restaurer le fichier**
- **Désinfecter puis restaurer le fichier**
- **Masquer les rapports dépendants**
- **Masquer les rapports lus**
- **Période**

4.3.14.2. Journaux d'infrastructure

L'onglet journaux d'infrastructure affiche des informations sur le statut des clients (statut des tâches d'analyse, statut de la mise à jour des signatures antivirales, etc.).

Un clic droit donne accès au menu contextuel suivant :

- **Rafraichir**
- **Supprimer**
- **Marquer comme lu** : marque le(s) rapport(s) sélectionné(s) comme lu.
- **Marquer comme non lu** : marque le(s) rapport(s) sélectionné(s) comme non lu.
- **Exporter les rapports**: export le(s) rapport(s) sélectionné(s) ou la liste entière en tant que fichier XML.

La barre d'outils de l'onglet journaux d'infrastructure donne accès aux options et filtres suivants :

- **Rafraîchir**
- **Supprimer**
- **Imprimer**
- **Affichage des pages**
- **Masquer les rapports lus**: masque les rapports lus
- **Période**

4.3.15. Protocoles (iOS)

Après avoir sélectionné un ou plusieurs clients iOS dans la rubrique **Clients**, l'onglet Protocoles affiche les détails relatifs au(x)client(s) iOS sélectionné(s). Les rapports contiennent des informations sur le statut, le déploiement des profils et les actions antivol.

- **Statut**: Statut du rapport.
- **Client**: Nom de l'appareil.
- **Date/heure**: Horodatage du rapport.

Un clic-droit sur un rapport puis **Supprimer** permet de le retirer de la liste.

4.3.16. Statistiques

Avec l'onglet Statistiques, vous consultez les informations relatives aux attaques de virus et aux tentatives d'infections des clients/e-mails sur le Serveur Exchange, ainsi que le statut de sécurité des

réseaux gérés. Différents affichages sont disponibles. Les informations peuvent être présentées sous forme de texte ou de graphique (histogramme et secteurs). Il est possible d'en modifier l'apparence avec la fonction **Affichage**. Des informations concernant les **Clients** (indisponible si un serveur Exchange est sélectionné), la **Méthode de détection**, la **Liste des virus** et la **Liste des infections bloquées** sont proposées.

4.4. Rubrique Serveur

La rubrique Serveur permet de configurer des serveurs ayant été sélectionnés sur les ManagementServers à la rubrique **Clients/ManagementServers**.

4.4.1. Serveur

L'onglet Serveur donne accès aux options et informations ManagementServer telles que la version, les journaux, la gestion des utilisateurs, etc.

4.4.1.1. Vue d'ensemble

Le sous-onglet Vue d'ensemble permet de vérifier les informations sur le statut des serveurs et pour installer et gérer les serveurs de sous réseau. Les informations disponibles sont les suivantes :

- **Nom** : nom du serveur
- **Type** : type de serveur (**Serveur principale**, **Serveur secondaire**, **Serveur de sous réseau**)
- **Serveur** : Nom du ManagementServer principal (uniquement pour les Serveurs de sous réseaux et Serveurs secondaires)
- **Nombre de clients** : le nombre de clients attribué au serveur.
- **Dernier accès** : horodatage de la dernière synchronisation avec le ManagementServer principal (uniquement pour les serveurs de sous-réseaux)
- **État des données** : dernière tentative de mise à jour des signatures antivirales.
- **Version** : version du serveur et sa date de sortie
- **Statut** : informations sur le statut du serveur tel que le statut de mise à jour.
- **Mise à jour programme** : Si une mise à jour est disponible pour un serveur de sous-réseau, le statut sera affiché ici.

Les options suivantes sont disponibles via la barre d'outils ou le menu contextuel (clic droit) :

- **Rafraîchir**
- **Assistant d'installation du serveur**
- **Supprimer** : supprime un ou plusieurs serveur(s) de sous-réseau de la liste. Ceci ne supprime pas le logiciel installé sur le serveur de sous-réseau.
- **Synchroniser** (uniquement via le menu contextuel) : déclenche manuellement la synchronisation des serveurs de sous réseaux.
- **Attribuer des clients** : vous pouvez assigner des clients ou des groupes de clients à des serveurs de sous-réseau. Ces derniers centralisent la communication des clients avec le serveur principal, ce qui minimise la charge réseau. Le groupement de clients avec un serveur de sous-réseau n'influe pas sur la composition des groupes de clients (créés dans la rubrique **Clients/ManagementServers**). Autrement dit, des clients qui ont été assignés à des serveurs de sous-réseau différents peuvent être regroupés dans un même groupe de clients.

- **Installer le serveur de sous-réseau** : ajoute un nouveau serveur de sous-réseau. Dans la boite de dialogue suivante, entrez le **Nom de l'ordinateur** du serveur de sous-réseau ou sélectionnez-le dans la liste des machines proposées. Saisissez un compte Administrateur lié à cet ordinateur et confirmez avec **OK** pour lancer l'installation distante. Celle-ci peut être visualisée en utilisant **Vue d'ensemble des installations**. Une installation d'un serveur de sous-réseau à distance est sujette aux mêmes prérequis qu'une **installation à distance de G DATA Security Client**. Les serveurs de sous-réseau utilisent Microsoft SQL Server 2014 Express, qui ne prend pas en charge Windows Vista et Windows Server 2008/2003. Sur ce type de système, les serveurs de sous-réseau peuvent être installés via l'option de serveur de sous-réseau de l'**installation locale** de G DATA ManagementServer.
- **Désinstaller le serveur** : lance une désinstallation à distance du serveur de sous-réseau sélectionné qui peut être surveillée grâce à la fenêtre **Vue d'ensemble des installations**.
- **Autoriser le serveur** : afin d'éviter que des serveurs de sous-réseau non autorisés n'accèdent au serveur de mise à jour, les serveurs de sous-réseau installés localement doivent être autorisés. C'est seulement après l'autorisation que le ManagementServer commence à synchroniser des données avec le serveur de sous-réseau.

  Les serveurs de sous-réseau qui ont été installés à distance à partir de la fonction **Ajouter un serveur de sous-réseau** sont automatiquement autorisés. Seuls les serveurs de sous-réseau installés localement et ceux mis à jour vers la version 13 doivent être autorisés manuellement. Les désinstallations distantes sont seulement possibles sur les serveurs de sous-réseaux autorisés.
- **Activer la mise à jour programme** (uniquement via le menu contextuel) : Les serveurs de sous-réseau avec la version 12 de ManagementServer requièrent une installation manuelle du serveur de la base de données, avant qu'ils puissent être mis à jour vers la version 14. Sur ces systèmes, installez en premier lieu Microsoft SQL Server 2014 Express (Windows Server 2008 R2 / Windows 7 et plus récent) ou Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista), ensuite utilisez l'option pour autorisation la mise à jour du programme. Après la mise à jour, utilisez GdmmsConfig.exe sur le serveur de sous-réseau pour configure la connexion à la base de données. Plus d'informations se trouvent dans le Référence Guide.
- **Propriétés** (uniquement via le menu contextuel) : Affiche une fiche d'informations sur le serveur sélectionné.

Assistant d'installation du serveur

L'assistant d'installation est automatiquement lancé au premier démarrage de G DATA Administrator, il est cependant toujours possible de l'exécuter via le menu **Admin**. Il vous guide pour effectuer des paramétrages essentiels pour le ManagementServer.

Tous les clients qui doivent être protégés par le logiciel G DATA doivent d'abord être activés. Les clients à activer doivent être sélectionnés, puis activés d'un clic sur **Activer**. Il est possible que certains ordinateurs ne soient pas présents dans la liste (parce qu'ils n'ont pas été allumés depuis longtemps ou qu'ils ne disposent pas de partage de fichiers ou d'imprimantes, par exemple). Pour activer ces clients, saisissez le nom de l'ordinateur dans le champ de saisie **Ordinateur**. Cliquez ensuite sur **Activer**, l'ordinateur à activer apparaît alors dans la liste des clients. Une fois tous les ordinateurs à protéger activés, vous pouvez accéder à l'étape suivante en cliquant sur **Suivant**. Une fois les clients activés, la case **Installer automatiquement le logiciel client sur les ordinateurs activés** est cochée. Si la distribution du logiciel doit avoir lieu à un moment ultérieur sur les ordinateurs clients, vous devez désactiver cette option en décochant la case.

Les prochaines étapes de l'assistant d'installation vous aident à configurer les paramétrages les plus fréquemment utilisés :

- **Mises à jour internet** : Configure les mises à jours des signatures antivirales et des fichiers programme. Se rendre à l'onglet **Mises à jour** pour plus d'information.
- **Notifications par e-mail** : Configure les paramètres du serveur de mail, les groupes d'emails aussi que les alertes. Plus d'informations disponibles dans **Paramètres généraux** > **Messagerie électronique**.
- **Paramètres pour les périphériques mobiles** : configuration pour le paramétrage des appareils Android. Plus d'informations disponible dans **Paramètres généraux** > **Android**.
- **Configuration pour l'accès au G DATA ActionCenter** : les identifiants ActionCenter sont nécessaires pour accéder à la gestion des appareils iOS et aux fonctions de Monitoring réseau. Plus d'information dans l'onglet **ActionCenter**.

Cliquer sur **Terminer** pour fermer l'assistant. Si vous avez choisi l'option **Installer automatiquement le logiciel client sur les ordinateurs activés**, l'assistant lancera l'installation distante de G DATA Security Client sur les machines activées.

4.4.1.2. Gestion des utilisateurs

En tant qu'administrateur système, vous pouvez attribuer d'autres droits d'accès utilisateur à l'interface G DATA Administrator. Pour ce faire, cliquez sur le bouton **Nouveau**, saisissez le **Nom d'utilisateur**, les **Autorisations** de l'utilisateur en question (Lire, Lire/écrire, Lire/écrire/restaurer les sauvegardes), définissez le **Type de compte** (**Connexion intégrée**, **Utilisateur Windows**, **Groupe d'utilisateurs Windows**) et saisissez un **Mot de passe** pour l'utilisateur.

4.4.1.3. Journaux d'infrastructure

L'onglet Journaux d'infrastructure affiche des informations sur l'état des serveurs (mises à jours des signatures/ programme…). La barre d'outils et le menu contextuel sont identiques à ceux disponible dans la rubrique Clients **Protocoles** > **Journaux d'infrastructure**.

4.4.2. Paramètres généraux

L'onglet Paramètres généraux permet de configurer certains paramètres tels que la synchronisation Client /servers ou Serveur/Serveurs de sous-réseaux, les dossiers d'enregistrement des sauvegardes etc.

4.4.2.1. Nettoyage

Sous **Nettoyer automatiquement**, indiquez le délai avant la suppression automatique de certains objets/informations :

- **Supprimer automatiquement les journaux d'infrastructure** : cette option vous permet de supprimer les entrées du journal après un certain nombre de jours.
- **Supprimer automatiquement le protocole d'analyse** : cette option vous permet de supprimer les journaux d'analyse qui datent de plus d'un certain nombre de jours.
- **Supprimer automatiquement les événements de sécurité** : cette option vous permet de supprimer les rapports après un certain nombre de mois.
- **Supprimer automatiquement l'historique des rapports** : cette option vous permet de supprimer l'historique des rapports après un certain nombre de mois.

- **Supprimer automatiquement les clients inactifs** : cette option vous permet de supprimer les clients qui ne se sont pas connectés au réseau depuis un certain nombre de jours.
- **Supprimer automatiquement les fichiers correctifs** : les fichiers des correctifs sont automatiquement supprimés après un certain temps.

4.4.2.2. Synchronisation

Dans la rubrique Synchronisation, vous pouvez définir l'intervalle de synchronisation entre ManagementServer principal et les : clients, serveurs de sous-réseau et Serveur Active Directory.

- **Clients**
  - **Fréquence de de synchronisation avec Management Serveur principal** : indiquez la fréquence à laquelle les clients doivent se connecter au serveur pour déterminer si de nouvelles mises à jour et de nouveaux paramètres sont disponibles. La valeur par défaut est cinq minutes.
  - **Informer les clients en cas de modification des options du serveur** : Cochez, cette case pour immédiatement informer les ordinateurs de se synchroniser sur le serveur, sans tenir compte de la fréquence de synchronisation définis.
  - **Limiter le nombre de connexions concurrentes sur le serveur** : Spécifiez le nom de clients qui peuvent se connecter simultanément sur le serveur de gestion. Le nombre de connexions dépend de spécifications du serveur et de l'infrastructure réseau. Si vous rencontrez des problèmes de performances, réduire ce nombre peut améliorer la situation.
- **Serveur de sous-réseau**
  - **Fréquence de synchronisation** : Définit la fréquence de synchronisation entre le MMS et le(s) serveur(s) de sous-réseau.
  - **Transmettre immédiatement les nouveaux rapports au serveur principal** : cochez cette case, pour immédiatement transmettre les nouveaux rapports au serveur principal, sans tenir compte de la fréquence de synchronisation définis.
- **Active Directory**
  - **Synchroniser régulièrement le répertoire actif** : Active la synchronisation entre Active Directory et le Management Server. La synchronisation ne peut s'effectuer que si un groupe au moins a été lié à Active Directory.
  - **Intervalle** : définissez la fréquence de la synchronisation entre Active Directory et G DATA ManagementServer. Si vous optez pour une synchronisation quotidienne, vous pouvez programmer l'heure précise à laquelle la synchronisation avec Active Directory se délenche.

4.4.2.3. Sauvegarde

La sauvegarde est un **module optionnel**.

Pour garantir le bon déroulement des tâches de sauvegarde, l'espace disque disponible doit être suffisant aussi bien au niveau du serveur (espace de sauvegarde) que du client (espace cache de sauvegarde). Lorsque l'espace disque libre du client ou du serveur descend en dessous du seuil d'alerte, un message d'avertissement est créé dans le module **Événements de sécurité**. La mémoire tampon du client est automatiquement nettoyée, tout en conservant la dernière sauvegarde mais en supprimant les autres (si elles ont été téléchargées sur le ManagementServer). Dans le cas où l'espace disque libre du client ou du serveur descend en dessous du seuil critique, un message d'erreur est créé dans le module **Événements de sécurité**. Dans ce cas, l'espace de sauvegarde du serveur ou du

client est alors automatiquement nettoyé. S'il n'y a toujours pas assez d'espace disque libre sur le serveur, les sauvegardes ne seront plus effectuées.

Sous **Répertoires de sauvegarde du côté du serveur**, vous pouvez indiquer le chemin d'enregistrement de toutes les sauvegardes effectuées. Si aucun répertoire n'est sélectionné, toutes les sauvegardes sont enregistrées sous C:\ProgramData\G DATA\AntiVirus ManagementServer \Backup ou C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Backup.

Toutes les sauvegardes créées avec le logiciel G DATA étant chiffrées, il est également possible d'exporter les mots de passe des sauvegardes et de les enregistrer pour les utiliser ultérieurement. Le bouton **Importer l'archive de sauvegarde** permet d'accéder aux sauvegardes enregistrées dans d'autres dossiers.

4.4.2.4. Messagerie électronique

G DATA ManagementServer peut automatiquement envoyer un message d'alerte pour certains évènements. . Activez la notification par email en sélectionnant les rapports appropriés (**Virus détectés**, **Demande de permission**, etc.). Sélectionnez les destinataires dans **Groupe(s) de destinataires**. L'option **Limitation** vous permet d'éviter un afflux trop important de courriers électroniques en cas d'attaque massive. Après avoir sélectionné un destinataire, cliquez sur **Déclencher l'alerte test** pour envoyer une alerte test.

Pour modifier les **paramètres des courriers électroniques**, cliquez sur le bouton des paramètres étendus ( ).

Paramètres des courriers électroniques
Indiquez ici le **Serveur SMTP** et le **Port** (le port 25 normalement) utilisés par G DATA ManagementServer pour l'envoi de courriers électroniques. Une adresse d'expéditeur (valide) est nécessaire à l'envoi de courriers électroniques. Si votre serveur SMTP requiert une authentification, cliquez sur **Authentification SMTP**. Vous pouvez configurer la procédure pour l'**Authentification SMTP** (connexion directe au serveur SMTP) ou pour l'authentification **SMTP après POP3**.

Sous **Groupe(s) de destinataires**, vous pouvez gérer les listes de destinataires (équipe de gestion, techniciens, etc.).

4.4.2.5. Android

L'onglet Android permet d'indiquer les données d'accès des appareils Android, tout comme ceux pour Firebase Cloud Messaging.

Sous **Authentification pour les clients Android**, saisissez un **Mot de passe** permettant d'authentifier l'appareil Android au niveau de l'application ManagementServer. Pour pouvoir exécuter des **Actions d'urgence** sur le périphérique mobile à partir du serveur, vous devez saisir l'**Identifiant de l'expéditeur** et la **Clé API** (Clé serveur) de votre compte de messagerie Firebase Cloud Messaging. Vous pouvez créer des comptes gratuits pour cette notification poussée sous **firebase.google.com**. Pour plus d'informations sur Firebase Cloud Messaging, reportez-vous au Guide de référence.

4.4.3. Mises à jour

Tous les clients possèdent une copie locale de la base de données des virus afin que la protection antivirus puisse être assurée, même hors ligne (c'est-à-dire lorsque le PC client n'est pas connecté à

G DATA ManagementServer ou à Internet). La mise à jour des fichiers sur les clients se déroule en deux étapes (toutes deux pouvant naturellement être automatisées). Au cours de la première étape, les fichiers provenant du serveur de mise à jour G DATA sont copiés dans un dossier de l'application G DATA ManagementServer. Au cours de la deuxième étape, les nouveaux fichiers sont distribués aux clients (reportez-vous à la rubrique de tâches **Paramètres du client** > **Généralités** > **Mises à jour**).

4.4.3.1. Mises à jour des signatures

L'onglet Mises à jour permet de configurer la façon dont s'effectue le téléchargement des mises à jour depuis les serveurs G DATA vers G DATA ManagementServer.

Les informations suivantes y sont disponibles :

- **Version du moteur A** : La version des signatures du moteur A disponible sur le ManagementServer
- **Version du moteur B** : la version des signatures du mateur B disponible sur le ManagementServer
- **Dernière exécution** : Horodatage de la dernière mise à jour effectuée.
- **Statut** : le statut de la dernière mise à jour effectuée.
- **Mettre le statut à jour** : si l'affichage ne reflète pas encore les modifications effectuées, ce bouton vous permet d'actualiser l'affichage du statut des signatures antivirus.
- **Démarrer la mise à jour maintenant** : le bouton Démarrer la mise à jour maintenant vous permet de procéder directement à une actualisation de la base de données des virus.

Pour automatiser la mise à jour des signatures antivirale cochez l'option **Procéder régulièrement à la mise à jour** et définissez quand ou à quelle fréquence la mise à jour doit être effectuée. Pour que la mise à jour s'effectue automatiquement G DATA ManagementServer doit avoir accès à Internet. Les identifiants et configuration proxy de l'onglet **Données d'accès et paramètres**, doivent être valides.

La distribution peut être assurée de manière centralisée (depuis le ManagementServer ou un serveur de sous-réseau vers les clients) ou, si **Déploiement de la mise à jour de poste à poste** est cochée, de manière décentralisée (permettant aux clients déjà mis à jour de distribuer les mises à jour vers les autres clients). Nous attirons votre attention sur le fait qu'il est possible que des modifications doivent être apportées à la **configuration des ports** pour la distribution des mises à jour.

4.4.3.2. Mises à jour du programme

L'onglet Mises à jour du programme permet de configurer la façon dont s'effectue le téléchargement des mises à jour programme depuis les serveurs G DATA vers G DATA ManagementServer.

Les informations et paramètres suivants sont disponibles dans la section Fichiers du programme (Clients) :

- **Version actuelle** : version des fichiers programme client disponibles sur le ManagementServer
- **Dernière exécution** : Horodatage de la dernière exécution de la mise à jour des fichiers programme
- **Statut** : le statut du processus de mise à jour
- **Mettre le statut à jour** : si l'affichage ne reflète pas encore les modifications effectuées, le bouton Rafraîchir vous permet d'actualiser l'affichage du statut de la version du logiciel.
- **Démarrer la mise à jour maintenant** : le bouton Démarrer la mise à jour maintenant vous

permet de procéder directement à une actualisation du logiciel client.

Les mises à jour Internet du logiciel client peuvent être exécutées automatiquement. Le paramétrage est identique à ceux effectué dans **Mise à jour des signatures**.

> G DATA ManagementServer peut uniquement être actualisée via le menu Démarrer de Windows. Pour actualiser les fichiers du programme G DATA ManagementServer, appelez l'utilitaire **Mise à jour Internet** dans le groupe de programmes G DATA ManagementServer du menu Démarrer.

4.4.3.3. Déploiement progressif

La rubrique **Déploiement progressif** vous permet de déterminer si les mises à jour du programme doivent être transmises à tous les clients en même temps ou de manière progressive. La distribution progressive permet de limiter la charge au niveau du système, charge qui est inévitable lors de telles mises à jour du programme.

Si vous optez pour une distribution progressive, vous pouvez indiquer si la distribution est effectuée automatiquement, déterminer un ordre de distribution des mises à jour du programme entre les clients et définir l'intervalle entre les différentes phases de distribution.

4.4.3.4. Données d'accès et paramètres

Lors de l'enregistrement en ligne, G DATA vous fait parvenir les données d'accès pour la mise à jour des bases de données antivirus et des fichiers du programme. Saisissez-les sous **Nom d'utilisateur** et **Mot de passe**. Sous **Région**, sélectionnez le serveur de mise à jour le plus proche pour garantir une vitesse optimale lors du téléchargement des mises à jour. L'option **Vérification de la version** activée par défaut doit généralement être activée pour garantir une vitesse de mise à jour optimale. Vous devez toutefois désactiver la vérification de la version si des problèmes surviennent au niveau des fichiers de la base de données de virus locale. L'intégrité de tous les fichiers de la base de données de virus est alors vérifiée lors de la mise à jour Internet suivante et les fichiers présentant des erreurs sont de nouveau téléchargés.

Cliquez sur le bouton **Paramètres proxy** pour ouvrir une fenêtre dans laquelle vous pouvez saisir les données d'accès pour Internet et le réseau. Vous ne devez modifier ces paramètres que si vous rencontrez des problèmes avec les paramètres standards du logiciel G DATA (en raison de l'utilisation d'un serveur proxy, par exemple) et si une mise à jour Internet ne peut être effectuée.

> Le logiciel G DATA peut utiliser les données d'accès de l'application Internet Explorer (à compter de la version 4). Commencez par configurer Internet Explorer, puis vérifiez que la page test de notre serveur de mise à jour est accessible : http://ieupdate.gdata.de/test.htm. Désactivez ensuite l'option **Utiliser le serveur proxy**. Sous **Compte utilisateur**, indiquez le compte pour lequel vous avez configuré Internet Explorer (le même que celui utilisé pour la connexion à votre ordinateur).

4.4.3.5. Restaurer la signature

En cas de fausses alertes ou de problèmes similaires, il peut être parfois utile de bloquer la mise à jour des signatures antivirus et d'utiliser à la place une des mises à jour précédentes. Sous **Retours en arrière**, indiquez le nombre de mises à jour de signatures antivirus que vous souhaitez conserver en réserve pour les retours en arrière. Les cinq dernières mises à jour des signatures du moteur sont conservées par défaut.

En cas de problèmes avec la mise à jour du moteur A ou B, l'administrateur réseau peut donc bloquer les mises à jour pendant un certain temps et distribuer automatiquement à la place les précédentes signatures antivirus aux clients et aux serveurs de sous-réseau.

> Aucun retour en arrière ne peut être effectué sur les clients non associés à l'application G DATA ManagementServer (par exemple, les ordinateurs portables lors de déplacements professionnels). Un blocage des nouvelles mises à jour transféré par le serveur au client ne peut pas être annulé sans contact avec le logiciel G DATA ManagementServer.

Les dernières mises à jour du moteur sont répertoriées sous **Mises à jour bloquées** pour le **Moteur** sélectionné. Sélectionnez la ou les mises à jour que vous souhaitez bloquer, puis cliquez sur **OK**. Ces mises à jour ne sont alors plus distribuées et les clients qui les ont précédemment reçues sont réinitialisés jusqu'à la dernière mise à jour non bloquée. Cette opération a lieu dès qu'ils se connectent à l'application ManagementServer. Vous pouvez également bloquer automatiquement les nouvelles mises à jour jusqu'à une certaine date. Les mises à jour ne sont lues sur les clients qu'à compter de cette date. Pour ce faire, utilisez la fonction **Bloquer les nouvelles mises à jour jusqu'à**.

4.4.4. ReportManager

Le module ReportManager vous permet de configurer des rapports programmés au sujet du statut de sécurité de votre système et de les envoyer aux destinataires sélectionnés.

La barre d'outils offre les possibilités suivantes :

- **Rafraîchir**
- **Supprimer**
- **Ajouter une nouvelle planification de rapport** : les fonctions sont détaillées dans **Définition du rapport**.

Les options **Importer/Exporter** vous permettent d'importer et/ou d'exporter les paramètres du rapport. Cliquez avec le bouton droit de la souris sur un ou plusieurs rapports. Vous pouvez ici les **Supprimer** ou, si vous sélectionnez **Exécuter immédiatement**, les exécuter immédiatement. Pour modifier un rapport, cliquez sur **Propriétés**.

4.4.4.1. Définition du rapport

Vous pouvez définir ici le **Nom** du rapport et indiquer la **Langue** dans laquelle il doit être créé. Sous les **Groupes de destinataires**, vous sélectionnez la liste des destinataires du rapport. Pour ce faire, vous pouvez utiliser les groupes créés sous **Paramètres généraux** > **Messagerie électronique** > **Paramètres des courriers électroniques**. Vous pouvez également définir ici de nouveaux groupes de destinataires. En outre, vous avez la possibilité d'ajouter des adresses électroniques supplémentaires pour le rapport (les adresses doivent être séparées par une virgule) dans le champ de saisie **Destinataires supplémentaires**.

S'il s'agit de rapports générés une fois seulement, vous pouvez définir l'heure à laquelle les rapports doivent être établis. Pour les rapports réguliers, vous pouvez indiquer quand et à quelle fréquence la notification doit avoir lieu.

Sous **Tous les jours**, vous pouvez indiquer, en renseignant le champ **Jours de la semaine**, si les rapports doivent être générés seulement les jours de la semaine, tous les deux jours ou le week-end, lorsque l'ordinateur n'est pas utilisé à des fins professionnelles, par exemple.

Pour définir le contenu du rapport, vous devez cliquer sur le bouton **Nouveau** sous **Modules sélectionnés** et activer un des modules de rapports disponibles. La disponibilité des modules varie en fonction de la solution G DATA que vous utilisez. Les modules pour la planification des rapports sont répartis en trois catégories : **Généralités client**, **Protection client** et **PatchManager**. Sélectionnez le module souhaité et configurez les paramètres dans la partie inférieure de la fenêtre :

- **Limite** : Pour certains modules, vous pouvez limiter la quantité d'information qui sera incluse dans le rapport.
- **Type de client** : Vous pouvez choisir le type de clients qui seront inclus dans le rapport (Windows, Linux, Mac).
- **Format d'édition** : Vous pouvez sélectionner un format de rendu spécifique pour chaque module. Les options proposées sont les suivantes : **Tableau**, **Diagramme courbe**, **Diagramme à colonnes (3D)** et **Camembert (3D)**. Nous attirons votre attention sur le fait que tous les formats de rendu ne sont pas pris en charge par tous les modules.
- **Période couverte** : Sélectionnez une période relative ou absolue que le rapport devra couvrir.

Cliquez sur **OK** pour ajouter les modules sélectionnés au rapport. Des boutons vous permettant de **Modifier** ou de **Supprimer** les modules sont mis à votre disposition. Une fois la sélection et le paramétrage des modules terminés, vous pouvez générer un exemple de rapport avec les paramètres définis sous **Aperçu**.

Une fois le rapport créé, il s'affiche dans la vue d'ensemble du module ReportManager et est envoyé aux destinataires sélectionnés. Pour afficher toutes les instances d'un rapport, il vous suffit de double-cliquer sur le rapport et d'ouvrir les rapports correspondants.

L'ordinateur sur lequel l'application G DATA Administrator est exécutée doit être équipé de l'application Internet Explorer version 8 ou supérieure pour afficher l'aperçu des rapports et les instances de rapports.

4.4.5. Gestion des licences

La section de gestion des licences vous offre une vue d'ensemble permanente du nombre de licences du logiciel G DATA utilisées au sein de votre réseau. Si vous avez besoin de davantage de licences, cliquez sur le bouton **Étendre les licences** pour entrer directement en relation avec G DATA.

Le bouton **Exporter** vous permet d'exporter les informations de licences sous forme de fichier texte.

4.4.6. ActionCenter

G DATA Administrator se connecte au G DATA ActionCenter pour gérer les appareils iOS. **Créez un compte** et entrez votre **Nom d'utilisateur** et **Mot de passe**.

L'utilisation de G DATA ActionCenter requiert une licence G DATA valide. Assurez-vous d'avoir entré les **Nom d'utilisateur** et **Mot de passe** des mises à jour Internet correctement dans l'onglet **Mises à jour** > **Données d'accès et paramètres**.

> La communication avec G DATA ActionCenter est basée sur des composantes qui ne sont disponibles qu'à partir de Windows Vista. Les options iOS Mobile Device Management et le Network Monitoring ne sont pas disponibles lorsque G DATA ManagementServer ou Administrator fonctionne sur une machine Windows XP ou Windows Server 2003.

5. G DATA WebAdministrator

Le logiciel G DATA WebAdministrator est un logiciel de commande Web pour l'application G DATA ManagementServer. Il vous permet de définir les paramètres de l'application G DATA ManagementServer via une interface Web, dans un navigateur.

5.1. G DATA WebAdministrator

Pour utiliser G DATA WebAdministrator, il vous suffit de cliquer sur l'icône G DATA WebAdministrator de votre bureau. Vous pouvez également lancer votre navigateur Internet et accéder à la page qui vous a été indiquée à la fin du processus d'installation. L'adresse URL est composée de l'adresse IP ou du nom de l'ordinateur sur lequel le système IIS est exécuté et sur lequel l'application WebAdministrator est installée, ainsi que du suffixe du dossier (par exemple, *http://10.0.2.150/GDAdmin/*). Si vous n'avez pas encore installé le plug-in de navigateur Microsoft Silverlight, vous serez invité à le télécharger.

Une page de connexion permettant d'accéder à G DATA WebAdministrator s'ouvre alors. Vous devez saisir vos données d'accès comme dans l'application G DATA Administrator classique et cliquer sur le bouton **OK**. L'utilisation et les fonctions de l'application G DATA WebAdministrator sont similaires à celles de l'application **G DATA Administrator**.

5.2. Utilisation du programme G DATA WebAdministrator

L'interface du programme G DATA WebAdministrator est très similaire à celle du programme G DATA Administrator. Une fois connecté, vous pouvez consulter le tableau de bord central, qui vous offre une vue d'ensemble du réseau, des clients et du statut de l'application G DATA ManagementServer.

Les fonctions des applications WebAdministrator et G DATA Administrator sont identiques. Elles sont expliquées en détail au chapitre **G DATA Administrator**.

6. G DATA MobileAdministrator

L'application G DATA MobileAdministrator est la version smartphone de l'interface du programme G DATA ManagementServer. Elle peut être utilisée pour modifier et mettre à jour rapidement les paramètres, elle est également optimisée pour l'utilisation avec des périphériques mobiles. Pour ce faire, les fonctions les plus importantes et les plus fréquemment utilisées du programme G DATA Administrator sont organisées de manière à pouvoir être utilisées dans une large palette d'environnements de smartphone différents.

6.1. Lancement de l'application G DATA MobileAdministrator

Une fois l'installation de l'application G DATA MobileAdministrator terminée, vous pouvez y accéder depuis n'importe quel navigateur. Pour ce faire, démarrez votre navigateur et sélectionnez l'adresse URL indiquée à la fin du processus d'installation. L'adresse URL est composée de l'adresse IP ou du nom de l'ordinateur sur lequel le système IIS est exécuté et sur lequel l'application WebAdministrator est installée, ainsi que du suffixe du dossier (par exemple, *http://10.0.2.150/GDMobileAdmin/*).

La page de connexion de l'application MobileAdministrator se rapproche beaucoup de celle des applications **G DATA Administrator** et **G DATA WebAdministrator**. Indiquez ici le **Serveur**, le **Nom d'utilisateur**, votre **Mot de passe** et la **Langue** souhaitée. Sélectionnez l'option **Authentification Windows** si vous souhaitez vous connecter à l'aide de vos codes d'accès (au domaine) ou l'option **Authentification intégrée** si vous souhaitez que vos codes d'accès soient directement gérés par l'administrateur. Si vous souhaitez que vos codes d'accès (mot de passe inclus) soient de nouveau accessibles lors de la prochaine ouverture de la page de connexion, sélectionnez **Enregistrer les données de l'utilisateur**.

6.2. Utilisation du programme G DATA MobileAdministrator

Une fois la connexion au programme G DATA MobileAdministrator établie, le menu principal s'affiche. Quatre options sont alors à votre disposition : **Tableau de bord**, **Rapports**, **Clients** et **ReportManager**. Pour quitter le programme, appuyez sur le bouton **Déconnexion** dans la partie supérieure droite.

6.2.1. Tableau de bord

Le tableau de bord de l'application G DATA MobileAdministrator vous permet de disposer d'une vue d'ensemble des principales statistiques de votre réseau. Vous avez ici, comme sur l'écran Tableau de bord de l'application G DATA Administrator, une vue d'ensemble du programme G DATA ManagementServer et de ses clients. Vous pouvez également afficher des statistiques au sujet des connexions client et des infections bloquées.

Sélectionnez **Statut de l'application G DATA Security** pour obtenir une vue d'ensemble précise du statut du serveur et des clients. L'application MobileAdministrator vous indique le nombre de clients équipés du programme G DATA Security Client et vous fournit des informations au sujet du statut d'actualisation des signatures antivirus et d'autres composants du programme (OutbreakShield, pare-feu et outil de surveillance, par exemple). Si vous ouvrez la sous-rubrique des signatures antivirus, vous pouvez également procéder directement à des retours en arrière du moteur. Le statut de l'application ManagementServer est indiqué en détail sous **Statut du serveur**.

D'autres statistiques sont disponibles sous **Communication Clients / Serveur** et **Dix principaux clients - infections bloquées**. Appuyez sur **Statut du rapport** pour afficher des informations au sujet des infections, des demandes et des rapports d'erreurs.

6.2.2. Rapports

L'écran Rapports regroupe les rapports au sujet des virus, des événements du pare-feu et des messages de l'application PolicyManager. Il s'agit ici d'une présentation optimisée pour les périphériques mobiles des informations de la rubrique **Événements de sécurité** de l'application G DATA Administrator.

Sous **Période**, indiquez si vous souhaitez afficher les rapports du jour précédent, des sept derniers jours ou du mois dernier. L'application MobileAdministrator affiche alors les catégories pour lesquelles il existe des rapports. Lorsque vous appuyez sur une des catégories, une vue d'ensemble des événements enregistrés s'affiche. Vous pouvez filtrer les rapports par nom.

6.2.3. Clients

L'application MobileAdministrator vous offre une vue d'ensemble précise des clients gérés par le programme G DATA ManagementServer. Pour chaque client, vous pouvez consulter des informations détaillées. Les principaux paramètres de sécurité peuvent être directement modifiés via l'application MobileAdministrator.

Au niveau de la vue d'ensemble, vous pouvez afficher la liste de tous les ordinateurs gérés par G DATA ManagementServer. Vous pouvez également filtrer cette liste par nom. Si vous sélectionnez un client précis, vous pouvez afficher des statistiques au sujet des versions et des mises à jour propres au client en question. Vous pouvez également modifier directement les paramètres de sécurité importants. Vous pouvez ainsi activer ou désactiver l'**Outil de surveillance**, indiquer si les contenus Internet (HTTP) doivent être ou non traités, activer ou désactiver l'**Analyse d'inactivité** et activer ou désactiver le **Pare-feu**.

Dans la rubrique **Clients**, vous pouvez contrôler et modifier les paramètres **Contrôle des applications**, **Contrôle des périphériques**, **Contrôle du contenu Web** et **Temps d'utilisation d'Internet**.

6.2.4. ReportManager

ReportManager est la version mobile de la rubrique **ReportManager** de l'application G DATA Administrator. Vous avez ici la possibilité de configurer, de programmer et d'afficher en aperçu des rapports.

Pour ajouter une nouvelle tâche de rapport, appuyez sur **Ajouter la planification**. Il vous suffit d'appuyer sur les rapports existants pour les sélectionner en vue de la modification. Vous avez également à votre disposition toutes les possibilités de paramétrage de la version bureau du programme ReportManager.

7. G DATA Security Client

G DATA Security Client assure la protection des clients Windows et exécute les tâches que G DATA ManagementServer lui attribue, en arrière-plan, sans interaction utilisateur. Les clients disposent de signatures antivirus et d'un programme local, grâce auxquels les tâches peuvent également être effectuées lors du fonctionnement hors ligne (pour les ordinateurs portables qui ne disposent pas d'une connexion permanente à l'application G DATA ManagementServer, par exemple).

Une fois le logiciel client installé, une icône de la barre de démarrage permet à l'utilisateur du client d'accéder aux fonctions de protection antivirus, indépendamment du planning de l'outil d'administration. En tant qu'administrateur, vous sélectionnez les fonctions à la disposition de l'utilisateur dans la rubrique **Paramètres du client** de l'application G DATA Administrator.

En cliquant avec le bouton droit de la souris sur l'icône G DATA Security Client, un menu contextuel s'affiche pour accéder à toutes les fonctions Security Client.

7.1. Analyse antivirus

Cette option permet à l'utilisateur de s'assurer, à l'aide de G DATA Security Client, de l'absence de virus sur son ordinateur, indépendamment des tâches programmées dans G DATA Administrator.

L'utilisateur peut vérifier des disquettes, des CD/DVD, la mémoire de l'ordinateur et la zone de démarrage automatique, ainsi que des fichiers ou des répertoires. Les utilisateurs d'ordinateurs portables qui connectent rarement leur ordinateur au réseau de l'entreprise peuvent ainsi également bloquer les attaques de virus qui visent le système. La fenêtre **Options** permet à l'utilisateur client de définir les actions à effectuer si un virus est détecté (déplacement du fichier dans la zone de quarantaine, par exemple).

> L'utilisateur peut également vérifier les fichiers et les répertoires à partir de l'Explorateur Windows, en les sélectionnant et en cliquant, dans le menu contextuel affiché à l'aide du bouton droit de la souris, sur la fonction **Vérifier les virus (G DATA AntiVirus)**.

Lors de l'analyse antivirus, les entrées suivantes sont ajoutées au menu contextuel :

- **Priorité de l'analyse antivirus** : l'utilisateur a ici la possibilité de définir la priorité de l'analyse antivirus. Lorsque l'option **Élevé** est sélectionnée, l'analyse antivirus est effectuée rapidement, ce qui peut ralentir l'utilisation des autres programmes de l'ordinateur. Avec l'option **Faible**, l'analyse antivirus dure plus longtemps. Il est cependant possible de continuer à travailler sur l'ordinateur client sans gêne pendant la vérification. Cette option n'est disponible que lorsque l'analyse antivirus est lancée localement.
- **Suspendre la vérification antivirus** : cette option permet à l'utilisateur de suspendre une analyse antivirus lancée localement. Les tâches d'analyse définies à partir de l'application G DATA ManagementServer ne peuvent être suspendues que si l'administrateur a activé l'option **L'utilisateur peut interrompre ou annuler la tâche** lors de la création de la tâche.
- **Annuler la vérification antivirus** : cette option permet à l'utilisateur d'annuler une analyse antivirus lancée localement. Les tâches d'analyse définies à partir de l'application G DATA ManagementServer ne peuvent être annulées que si l'administrateur a activé l'option **L'utilisateur peut interrompre ou annuler la tâche** lors de la création de la tâche.
- **Afficher la fenêtre d'analyse** : l'utilisateur peut afficher la fenêtre d'informations dans laquelle le déroulement et la progression de l'analyse antivirus sont indiqués. Cette option n'est

disponible que lorsque l'analyse antivirus est lancée localement.

Vous pouvez activer ou désactiver l'option Analyse antivirus dans l'application G DATA Administrator, sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

7.2. Désactiver le gardien

Cette commande permet à l'utilisateur de désactiver l'outil de surveillance G DATA pour un délai défini (**5 minutes ... Jusqu'au redémarrage de l'ordinateur**). La désactivation temporaire peut être pratique si vous prévoyez de copier un grand nombre de fichiers, car cela permet d'accélérer le processus de copie. La protection antivirus en temps réel est en revanche désactivée pendant cette période.

Vous pouvez activer ou désactiver l'option Désactiver le gardien dans l'application G DATA Administrator, sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

7.3. Options

L'utilisateur de l'ordinateur client a la possibilité de modifier des paramètres dans les rubriques suivantes du client : **Gardien**, **Courriel**, **Analyse antivirus** (locale), **Filtre Web** et **Filtre antispam**. De cette manière, tous les mécanismes de protection du logiciel G DATA peuvent être désactivés sur le client. Cette option doit uniquement être mise à la disposition des utilisateurs expérimentés. Les différentes possibilités de paramétrage sont détaillées dans la rubrique **Paramètres du client**.

Vous pouvez activer ou désactiver les différents onglets dans l'application G DATA Administrator, sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

7.4. Quarantaine

Chaque client possède un dossier de quarantaine local, dans lequel les fichiers infectés (en fonction des réglages de l'outil de surveillance/la tâche d'analyse) peuvent être placés. Un fichier qui a été mis en quarantaine ne peut pas exécuter de routines nuisibles, même s'il contient un virus. Les fichiers infectés sont automatiquement compressés et verrouillés lors de la mise en quarantaine. Les fichiers destinés à la quarantaine, dont la taille est supérieure à 1 Mo, sont toujours consignés dans la quarantaine locale du client pour ne pas solliciter inutilement le réseau en cas d'attaque massive par des virus. Tous les fichiers dont la taille est inférieure à 1 Mo sont placés dans le dossier de quarantaine de l'application G DATA ManagementServer. Ces paramètres ne peuvent pas être modifiés. Pour plus d'information concernant les dossiers de la quarantaine vous rendre au chapitre **Emplacements d'enregistrement et chemins d'accès par défaut**.

Si un fichier infecté dont la taille est inférieure à 1 Mo est détecté sur un client mobile sans connexion à G DATA ManagementServer, il est alors enregistré dans la quarantaine locale et n'est placé dans la quarantaine de G DATA ManagementServer que lors de la connexion suivante. Une tentative de désinfection des fichiers dans le dossier de quarantaine peut être demandée. Si cela ne fonctionne pas, les fichiers peuvent être supprimés ou, le cas échéant, déplacés de la quarantaine vers leur emplacement d'origine.

> **Attention** : un retour ne supprime pas le virus. Choisissez cette option uniquement si le programme est incapable de fonctionner sans le fichier infecté et que vous en avez besoin pour récupérer des données.

Vous pouvez activer ou désactiver l'option Quarantaine dans l'application G DATA Administrator, sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

7.5. Mises à jour/Correctifs

Le module PatchManager est un **module optionnel**.

L'option Mises à jour/Patchs vous propose une vue d'ensemble des mises à jour et des correctifs du PC client.

L'onglet **Installé** répertorie l'ensemble des correctifs et des mises à jour installés sur le système. Double-cliquez sur une entrée pour obtenir des informations détaillées au sujet du correctif ou de la mise à jour. En cas de problèmes avec un correctif ou une mise à jour, l'utilisateur peut sélectionner le programme à l'aide du bouton **Désinstaller** et proposer ainsi automatiquement la désinstallation du programme à l'administrateur. Le **Statut** du correctif/de la mise à jour est alors actualisé en conséquence et l'administrateur reçoit un **rapport** avec une demande de retour en arrière. Indépendamment des éventuelles tâches de détection du logiciel définies à distance ou programmées, l'utilisateur peut rechercher des correctifs pour le système à l'aide du bouton **Vérifier les mises à jour**.

L'onglet **Disponible** affiche tous les logiciels, tous les correctifs et toutes les mises à jour disponibles pour le client. Double-cliquez sur une entrée pour obtenir des informations détaillées au sujet du correctif ou de la mise à jour. Pour lancer l'installation de données actualisées du programme en tant qu'utilisateur client, vous pouvez cliquer sur **Installer**. Le **Statut** du correctif/de la mise à jour est alors actualisé en conséquence et l'administrateur reçoit un **rapport** avec une demande de distribution.

Vous pouvez activer ou désactiver l'option Mises à jour/Patchs dans l'application G DATA Administrator, sous **PatchManager** > **Paramètres**.

7.6. Mise à jour Internet

Le logiciel G DATA Security Client permet d'effectuer des mises à jour Internet des signatures antivirus à partir d'ordinateurs clients en l'absence de connexion à l'application G DATA ManagementServer (voir **Paramètres du client** > **Généralités** > **Mises à jour**).

Vous pouvez activer ou désactiver l'option Mise à jour Internet dans l'application G DATA Administrator, sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

7.7. Désactiver le pare-feu

Le module Pare-feu est disponible dans les **solutions** Client Security Business, Endpoint Protection Business et Managed Endpoint Security.

L'option Désactiver le pare-feu permet de désactiver le pare-feu, même lorsque le client se trouve encore sur le réseau de l'application ManagementServer. Une fois le pare-feu désactivé, il est possible de le réactiver à l'aide de l'option **Activer pare-feu**.

Vous pouvez activer ou désactiver l'option Désactiver le pare-feu dans l'application G DATA Administrator, sous **Pare-feu** > **Vue d'ensemble** > **Fonctionnement au sein du réseau interne** > **L'utilisateur peut activer et désactiver le pare-feu**.

7.8. Pare-feu

Le module Pare-feu est disponible dans les **solutions** Client Security Business, Endpoint Protection Business et Managed Endpoint Security.

L'option Pare-feu ouvre l'interface du pare-feu. Dans la mesure où le client se trouve sur le réseau de l'application G DATA ManagementServer, le pare-feu sera géré de manière centralisée à partir du serveur. Dès que le client se connecte à un autre réseau (si vous utilisez un portable de l'entreprise chez vous, par exemple), l'interface du pare-feu peut être utilisée pour modifier la configuration hors site.

Vous pouvez activer ou désactiver l'option Pare-feu dans l'application G DATA Administrator, sous **Pare-feu** > **Vue d'ensemble** > **Fonctionnement hors du réseau interne** > **L'utilisateur peut modifier la configuration hors site**).

7.8.1. État

L'interface du pare-feu contient les informations de base concernant l'état actuel du pare-feu. Double-cliquez sur l'entrée correspondante pour exécuter des tâches ou passer à la rubrique concernée.

- **Sécurité** : désactiver ou activer le pare-feu. Uniquement disponible si l'option a été activée dans G DATA Administrator (**Pare-feu** > **Vue d'ensemble** > **Fonctionnement au sein du réseau interne** > **L'utilisateur peut activer et désactiver le pare-feu**).
- **Mode** : Le pare-feu peut être configuré soit en mode automatique (pilote automatique) soit en mode manuel (ensemble de règles). L'option peut être modifiée par le client seulement si le client est en dehors du réseau ManagementServer et si l'option a été activée dans G DATA Administrator (**Pare-feu** > **Vue d'ensemble** > **Fonctionnement hors du réseau interne** > **L'utilisateur peut modifier la configuration hors site**).
- **Réseaux** : Ouvre l'interface **Réseaux** qui recense les réseaux auxquels l'ordinateur est connecté et l'ensemble de règles utilisé.
- **Attaques repoussées** : dès que le pare-feu enregistre une attaque sur votre ordinateur, l'attaque est bloquée et enregistrée à cet endroit.
- **Radar d'applications** : cette boîte de dialogue vous indique les programmes momentanément bloqués par le pare-feu. Si vous souhaitez toutefois autoriser l'une des applications bloquées à exploiter le réseau, il suffit de la sélectionner et de cliquer sur le bouton **Autoriser**.

7.8.2. Réseaux

La rubrique Réseaux recense les réseaux auxquels votre ordinateur est connecté. Elle indique également l'ensemble de règles appliqué au réseau. Pour consulter ou modifier les paramètres définis pour un réseau, sélectionnez le réseau et cliquez sur le bouton **Modifier**. Les paramètres réseau ne peuvent être modifiés que si cela a été autorisé (**Pare-feu** > **Vue d'ensemble** > **Fonctionnement au sein du réseau interne** > **L'utilisateur peut activer et désactiver le pare-feu**) ou si le périphérique est en mode hors site (**Pare-feu** > **Vue d'ensemble** > **Fonctionnement hors du réseau interne** > **L'utilisateur peut modifier la configuration hors site**).

- **Informations relatives au réseau** : affiche des informations relatives au réseau, telles que, le cas échéant, l'adresse IP, le masque de sous-réseau, la passerelle standard, le serveur DNS et le serveur WINS.
- **Pare-feu actif sur ce réseau** : désactiver ou activer le pare-feu.
- **Utilisation partagée de la connexion Internet** : autorise le partage de connexion internet.
- **Autoriser les configurations automatiques (DHCP)** : autorise la configuration DHCP.
- **Jeu de règles** : Sélectionnez un **Jeu de règles** défini à appliquer à cette connexion. Cliquez sur **Modifier le jeu de règles** pour ouvrir l'**Assistant de règles**.

7.8.3. Jeux de règles

Grâce au module Jeux de règles, vous pouvez créer et modifier des jeux de règles (jeu de règles du pare feu à appliquer aux réseaux).

- **Nouveau** : créer un nouvel ensemble de règles. Dans la fenêtre suivante, entrer un **Nom du jeu de règles** et décider si l'ensemble de règles doit être pré-rempli avec les règles par défaut pour les réseaux fiables, non fiables et à bloquer.
- **Supprimer** : Supprime le jeu de règles sélectionné. Les règles par défaut ne peuvent pas être supprimées.
- **Modifier** : Modifie le jeu de règles sélectionné en utilisant l'**Assistant de règles**.

Le pare-feu met à votre disposition des jeux de règles prédéfinies applicables aux types de réseaux suivants :

- **Connexion directe à l'Internet** : les règles qui gèrent l'accès direct à Internet relèvent de cette catégorie.
- **Réseaux non fiables** : concerne généralement les réseaux ouverts qui accèdent à Internet.
- **Réseaux fiables** : sont généralement considérés comme réseaux fiables : les réseaux domestiques et les réseaux d'entreprise.
- **Réseaux à bloquer** : utilisez cette option pour bloquer provisoirement ou définitivement l'accès de votre ordinateur à un réseau.

7.8.3.1. Assistant de règles

L'assistant de règles vous permet d'ajouter de nouvelles règles ou de modifier les règles existantes d'un jeu de règles. L'assistant de règles est spécialement conçu pour les utilisateurs qui ne connaissent pas bien la technologie des pare-feux. Pour un contrôle plus détaillé sur les règles individuelles, utilisez l'**Éditeur de règles complet**.

L'assistant de règles propose diverses règles. Chacune d'elles peut autoriser ou interdire rapidement un type de trafic spécifique. Pour la plupart des règles, un sens spécifique peut être défini, c'est-à-dire qu'il détermine si le programme doit être bloqué pour les connexions entrantes, sortantes ou pour les deux.

- **Autoriser ou bloquer les applications** : vous permet de sélectionner une application sur votre disque dur et de lui autoriser ou lui interdire l'accès au réseau défini dans le jeu de règles.
- **Autoriser ou bloquer les services réseau** : le blocage d'un ou plusieurs ports peut donc permettre de combler des failles de sécurité que les hackers pourraient utiliser pour lancer des attaques. L'assistant vous permet de bloquer les ports de votre choix entièrement ou uniquement pour une application définie.
- **Partage de fichiers/d'imprimantes** : autorise ou interdit le partage de fichiers et d'imprimantes.
- **Autoriser ou bloquer les services de domaines** : autorise ou bloque les services de domaines.
- **Utilisation commune de la connexion Internet** : autorise ou bloque le partage de connexion internet (ICS).
- **Autoriser ou bloquer les services de réseau privé virtuel** : autorise ou bloque les services de réseau privé virtuel (VPN).

- **Éditeur de règles complet (mode expert)** : ouvre l'**Éditeur de règles complet**.

7.8.3.2. Éditeur de règles complet

Les plus experts peuvent utiliser l'Éditeur de règles complet. Il permet de définir des règles personnalisées pour les différents réseaux. Vous pouvez y créer les mêmes règles que dans l'Assistant des règles et définir des paramètres supplémentaires.

La fenêtre de l'Éditeur de règles complet ressemble à celle de l'**Ensembles de règles** du module **Pare-feu** de G DATA Administrator. On l'utilise pour créer, modifier, supprimer et classer des règles dans l'ensemble de règles. En plus des options disponibles dans G DATA Administrator, l'Éditeur de règles complet offre les options suivantes :

- **Action si aucune règle ne s'applique** : Définir l'action quand aucune règle existante n'est appliquée à un type de communication : **Autoriser**, **Refuser** ou **Interroger l'utilisateur**.
- **Mode adaptatif** : le mode adaptatif prend en charge les applications employant la technique du canal retour (FTP et de nombreux jeux en ligne, par exemple). Les applications de ce type se connectent à un ordinateur distant et établissent avec ce dernier un canal retour par l'intermédiaire duquel l'ordinateur distant se connecte à son tour à votre application. Si le mode adaptatif est activé, le pare-feu reconnaît cette voie de retour et l'autorise sans vous en avertir.
- **Réinitialiser** : Supprime toutes les modifications des jeux de règles, tout comme les règles automatiques.

En double-cliquant sur une règle ou en cliquant sur le bouton **Modifier**, vous pouvez modifier les lois individuelles. L'éditeur de règles individuelles correspond à la fenêtre **Modifier une règle** dans G DATA Administrator.

7.8.4. Journaux

Le module Journaux propose une vue d'ensemble détaillée de toutes les connexions entrants et sortantes. On peut l'utiliser pour vérifier le protocole de connexion, initialiser une application, un sens, un port local, un hébergeur à distance, isoler un port pour décider si les connexions sont interdites ou permises.

Cliquez sur **Supprimer** pour supprimer l'entrée du journal sélectionnée ou sur **Supprimer tout** pour supprimer complètement le journal. Le bouton **Détail** donne accès à plus d'informations sur l'entrée du journal sélectionné.

Avec un clic droit sur une entrée, vous avez accès à toutes les options. En plus de la vue **Détails**, ces options permettent de créer une nouvelle règle basée sur une entrée du journal, modifier une règle bloquant ou permettant une connexion, et mettre en place une vue filtrée du module des journaux.

7.8.5. Réglages

L'interface Réglages peut seulement être utilisée si la permission a été accordée dans G DATA Administrator (**Pare-feu** > **Vue d'ensemble** > **Fonctionnement au sein du réseau interne** > **L'utilisateur peut activer et désactiver le pare-feu** et **Pare-feu** > **Vue d'ensemble** > **Fonctionnement hors du réseau interne** > **L'utilisateur peut modifier la configuration hors site**).

- **Sécurité**: désactiver ou activer le pare-feu.
- **Mode**: le pare-feu peut être exécuté en mode automatique (pilote automatique) ou en mode

manuel (jeux de règles).

8. G DATA Security Client pour Linux

G DATA Security Client pour Linux s'exécute en tâche de fond et fournit des possibilités d'analyses antivirus. Pour les serveurs Linux, les modules optionnels Samba, Sendmail/Postfix et Squid sont disponibles (voir **Installer G DATA Security Client pour Linux**).

G DATA Security Client pour Linux est constitué d'une **interface utilisateur graphique (GUI)** et d'**applications en lignes de commandes**.

8.1. Interface utilisateur graphique (GUI)

Un raccourci vers l'interface utilisateur graphique (GUI) de G DATA Security Client pour Linux est disponible dans le menu des applications ou un menu analogue en fonction de la distribution Linux. Vous pouvez également lancer l'interface en exécutant */opt/gdata/bin/gdavclient-qt*.

Après le démarrage de l'application, faites un clic droit sur l'icône G DATA Security Client pour Linux afin d'ouvrir le menu contextuel qui donne accès à toutes les fonctions. Il est nécessaire de définir et d'autoriser les options disponibles en utilisant le module **Paramètres Client** de G DATA Administrator.

Cliquez sur l'icône dans la barre des tâches ouvre le menu contextuel qui permet l'accès à un des paramètres suivants :

- **Analyse antivirus**
- **Quarantaine**
- **Mise à jour**
- **Aide**
- **Ouvrir G DATA Security Client** : Ouvre l'interface graphique à la rubrique **Statut**.
- **À propos de G DATA Security Client**

Tous les modules peuvent être protégés contre la modification des paramètres (voir **Paramètres du client** > **Généralités** > **Fonctions du client**). Si la protection par mot de passe est activée, il faut cliquer sur le cadenas, en bas à gauche, et entrer le mot de passe pour modifier les paramètres.

8.1.1. Statut

Dans la rubrique Statut

- **Dernière analyse** : la date et l'heure de la dernière **Analyse antivirus** effectuée. Le bouton **Analyser l'ordinateur maintenant** lance une analyse complète de l'ordinateur.
- **Dernière mise à jour** : la date et l'heure de la dernière **Mise à jour**. Le bouton **Mettre à jour maintenant**, initie la mise à jour des signatures antivirales.

8.1.2. Analyse antivirus

L'option d'analyse antivirus vous permet d'analyser un ou plusieurs ou l'ordinateur entier. Si un virus est détecté, le client exécutera automatiquement l'action définie dans la section **Paramètres**. G DATA ManagementServer recevra une notification et un rapport sera ajouté au module **Événements de sécurité**.

Choisir une des actions suivantes pour lancer une analyse :

- **Analyser tout le système** : Effectue une analyse complète du système.
- **Analyser le secteur de lancement (bootsector)** : Effectue une analyse des secteurs de démarrage de la machine.
- **Analyser des fichiers et dossiers** : Effectue l'analyse des dossiers et fichiers sélectionnés dans périma

Les paramètres peuvent être configurés :

- **Réaction aux fichiers infectés** : Définit l'action à mener lorsque l'analyse antivirus détecte un fichier infecté.
  - **Uniquement faire apparaitre dans les fichiers journaux** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Désinfecter** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Supprimer** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Déplacer en quarantaine** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Demander à l'utilisateur** : Affiche un avertissement à l'utilisateur pour lui donner le choix de l'action à effectuer.
- **Si la désinfection ne fonctionne pas** : Lorsque **Désinfecter** a été sélectionné précédemment mais que la désinfection n'a pas eu être effectuée, alors une action alternative sera exécutée.
- **Réaction aux archives infectées** : Définit l'action à mener lorsque l'analyse antivirus détecte une archive infectée.
- **Type de fichiers** (voir **Tâches** > **Tâches d'analyse** > **Scanner**).

Dans la section **Avancé**, les options suivantes sont disponibles :

- **Heuristiques** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Analyser le secteur de lancement (bootsector)** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Vérifier les archives** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Taille maximale des archives** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Taille maximale des fichiers** : indiquez la taille maximale des fichiers analysés. Au-delà de cette taille les fichiers ne seront pas analysés.

La section **Exceptions** permet d'exclure dossiers et fichiers qui ne doivent pas être analysés.

L'autorisation d'accès au menu d'analyse s'effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L'utilisateur peut procéder aux analyses antivirus**).

8.1.3. Mise à jour

Le module Mise à jour s'assure que G DATA Security Client pour Linux dispose des dernières versions de signatures antivirales pour une protection optimale.

La date et l'heure de la dernière mise à jour des signatures s'affichent au niveau de **Dernière mise à jour**. La version exacte de chaque moteur s'affiche au niveau de **Moteur A** et **Moteur B**. Cliquez sur **Mise à jour des signatures antivirus** pour immédiatement lancer le processus de mise à jour.

Les paramètres des mises à jour de signatures antivirus sont disponibles dans **Paramètres** :

- **Source de la mise à jour des signatures** : définit si les clients doivent récupérer leurs mises à jour depuis le serveur ManagementServer local ou depuis les serveurs de mises à jour de G DATA sur internet (voir **Paramètres du client** > **Généralités** > **Mises à jour**).
- **Planification de la mise à jour** : définit la fréquence à laquelle doivent s'effectuer les mises à jour
- **Serveur Proxy** : paramétrages des informations pour accéder à internet via un serveur proxy si besoin
- **Données d'accès** : identifiants nécessaire pour pouvoir effectuer les mises à jour directement sur les serveurs G DATA sur internet

Les paramètres **Planification des mises à jour**, **Serveur Proxy** et **Données d'accès** ne sont utilisés que si **Charger les mises à jour antivirus depuis le ManagementServer** n'a pas été sélectionné sous **Source de la mise à jour des signatures** (voir **Paramètres du client** > **Généralités** > **Mises à jour**).

L'autorisation d'accès au menu Mises à jour des signatures antivirus s'effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L'utilisateur peut télécharger les mises à jour des signatures**)

8.1.4. Quarantaine

L'onglet Quarantaine affiche les objets ayant été placés en quarantaine par une **analyse antivirus**.

Pour chaque objet les informations suivantes sont disponibles :

- **Nom du fichier** : Indique le nom et l'emplacement de l'objet
- **Nom du virus** : Indique le nom du virus qui a infecté l'objet.
- **Taille du fichier** : Indique la taille de l'objet infecté.

Sélectionnez un ou plusieurs éléments et cliquez sur l'un des boutons suivants :

- **Désinfecter et restaurer** : Nettoie l'objet puis le replace à son emplacement d'origine.
- **Restaurer** : replace l'objet à son emplacement d'origine. Attention si l'objet n'est pas d'abord désinfecté il risque de propager l'infection !
- **Supprimer** : Supprime l'objet de la quarantaine.

L'autorisation d'accès au menu **Quarantaine** s'effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L'utilisateur peut afficher la quarantaine locale**)

8.1.5. À propos de G DATA Security Client

La fenêtre A propos affiche le statut d'informations à propos de G DATA Security Client pour Linux et peut seulement être ouverte à partir de l'icône de la barre de tâche. Elle affiche les informations suivantes :

- **Version** : La version du client installé
- **ManagementServer** : L'état actuel de la connexion au ManagementServer
- **Statut du logiciel de Sécurité** : Le statut des services d'arrière-plan du client.

8.2. Interface de ligne de commandes

Comme alternative à l'interface graphique, une interface en ligne de commandes est disponible pour configure et exécuter G DATA Security Client pour Linux. **Gdavclient-cli** sert à exécuter des analyses et mettre à jour les signatures antivirales. **gdavclientc** permet de configurer et lancer des analyse, afficher les informations de version, de télécharge les mises à jour de signatures antivirus et de gérer le démon du serveur. Les deux applications doivent être exécutées en tant que root pour assurer le plein accès aux fichiers système.

8.2.1. gdavclient-cli

Par défaut gdavclient-cli se trouve dans le dossier /usr/bin. La syntaxe suivante est à utiliser pour exécuter gdavclient-cli : *gdavclient-cli [<option>] <emplacement du fichier>*. Les options suivantes sont disponibles :

- **--status** : affiche le statut des démons gdavclientd et gdavserver.
- **--version** : Affiche les informations de version
- **--mmsconnection** : affiche les informations concernant la connexion à G DATA ManagementServer
- **--lastscan** : Affiche le journal de la dernière analyse
- **--lastupdate** : affiche les informations concernant la dernière mise à jour des signatures antivirales.
- **--update** : met à jour les signatures antivirales.
- **--sysinfo** : crée un fichier appelé gdatahwinfo-<Date>.tar.gz, qui contient des fichiers debug tels que des fichiers journaux et des fichiers de configuration.

Lorsqu'un chemin vers in dossier ou un fichier est indiqué, gdavclient-cli lance une analyse antivirus.

8.2.2. gdavclientc

Par défaut, gdavclientc est localisé dans le dossier /usr/bin. Il est indépendant de G DATA ManagementServer et récupère ses valeurs de configuration depuis /etc/gdata/gdav.ini. La syntaxe pour gdavclientc est la suivante : *gdavclientc [<options>] <commande>*.

Voici les commandes qui peuvent être utilisées:

scan:<path>: Initialise une analyse de(s) fichier(s) à *<path>*et retourne le résultat. *<path>*peut être un chemin absolu ou relative vers un fichier ou un dossier (qui sera scanné de façon récurrente). L'utilisation de caractères de remplacement (***, *?*) est autorisée.

scanboot: Exécute une analyse des zones de boot. Tous les médias non-optiques qui sont listés sous /proc/partitions seront scannés.

abort: Arrête l'analyse en cours.

start: Démarre gdavserver.

stop: Arrête gdavserver.

restart: Arrête et redémarre gdavserver.

updateVDB<:moteur>: lance la mise à jour du moteur A ou du moteur B. Une fois la mise à jour terminée, le démon du serveur doit être relancé

dump: Affiche les configurations actuelles.

set:<key>=<value>: Active une option spécifique dans la configuration de gdavserver, écrasant ainsi

l'option existante (récupéré depuis /etc/gdata/gdav.ini). Ces options sont activées temporairement et sont perdues à l'arrêt de gdavserver.

get:<key>: Affiche les valeurs actuelles de l'option spécifique de configuration de gdavserver.

reload: Recharge toutes les valeurs depuis /etc/gdata/gdav.ini.

engines: Liste le nom de tous les moteurs utilisés.

baseinfo: Affiche les informations de la version.

coreinfo: Affiche les informations des moteurs antivirus.

pid: Affiche le PID de gdavserver.

Si vous utilisez la commande **scan:** pour exécuter une analyse antivirale, les options suivantes peuvent être utilisées :

-s: En plus des informations fournies par l'analyse régulière, un récapitulatif des résultats de l'analyse sera affichée.

-x: En plus des informations fournies par l'analyse régulière, un récapitulatif des résultats de l'analyse sera affichée au format XML.

9. G DATA Security Client pour Mac

G DATA Security Client pour Mac permet de protéger les machines Mac. Il permet d'effectuer des analyses antivirus programmées ou à la demande et protège en temps réel grâce au Gardien.

Après l'**installation de l'application**, une icône apparait dans la barre de menu. Il est nécessaire de définir et d'autoriser les options disponibles en utilisant le module **Paramètres Client** de G DATA Administrator.

Cliquez sur l'icône dans la barre de menu ouvre le menu contextuel qui permet l'accès à un des paramètres suivants :

- **Activer/désactiver Gardien**
- **Analyse antivirus**
- **Quarantaine**
- **Mise à jour**
- **Aide**
- **Ouvrir G DATA Security Client** : Ouvre l'interface graphique à la rubrique **Statut**.
- **À propos de G DATA Security Client**

Tous les modules sont protégés contre des changements imprévus. Cliquez sur le cadenas, en bas à gauche, pour déverrouiller la possibilité de modification des paramètres. Si les droits root sont nécessaires l'utilisateur devra saisir des identifiants.

9.1. Statut

Dans la rubrique statut vous avez un aperçu rapide de l'état de la protection du client. L'icône de la barre de menu peut être utilisée pour évaluer s'il existe un risque immédiat pour le client.

- **Gardien** : indique l'état du **Gardien**. Il peut être temporairement désactivé en utilisant le menu déroulant
- **Dernière analyse** : la date et l'heure de la dernière **Analyse antivirus** effectuée. Le bouton **Analyser l'ordinateur maintenant** lance une analyse complète de l'ordinateur.
- **Dernière mise à jour** : la date et l'heure de la dernière **Mise à jour**. Le bouton **Mettre à jour maintenant**, initie la mise à jour des signatures antivirales.

9.2. Gardien

Le gardien fonctionne en tâche de fond pour analyser les fichiers et agir lors de la détection d'un malware.

Les paramètres peuvent être configurés :

- **Statut**
  - **Activer le gardien** : Active le gardien (recommandé)
  - **Désactiver le gardien** : Désactive le gardien de manière permanente. Attention : la désactivation du gardien met en danger la machine.
  - **Désactiver le gardien jusqu'au prochain démarrage** : Désactive le gardien qui sera automatiquement relancé au redémarrage de la machine.

  - **Désactiver le gardien pour … minutes** : Désactive le gardien pour le temps spécifié. Le gardien est automatiquement relancé à la fin de la période défini.
- **Réaction aux fichiers infectés** : Permet de choisir l'action à faire lors de la découverte d'un malware par le Gardien.
  - **Uniquement faire apparaitre dans les fichiers journaux** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Désinfecter** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Supprimer** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Déplacer en quarantaine** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
  - **Demander à l'utilisateur** : Affiche un avertissement à l'utilisateur pour lui donner le choix de l'action à effectuer.
- **Si la désinfection ne fonctionne pas** : Lorsque Désinfecter a été sélectionné précédemment mais que la désinfection n'a pas eu être effectuée, une action alternative sera exécutée.
- **Réaction aux archives infectées** : Permet de choisir l'action à faire lorsque le Gardien découvre un malware dans une archive.
- **Type de fichiers** (voir **Tâches** > **Tâches d'analyse** > **Scanner**)

Dans la section **Avancé**, les options suivantes sont disponibles :

- **Heuristiques** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Analyser le secteur de lancement (bootsector)** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Vérifier les archives** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Taille maximale des archives** (voir **Paramètres du Client** > **Gardien** > **Paramètres**)
- **Taille maximale des fichiers** : indiquez la taille maximale des fichiers analysés. Au-delà de cette taille les fichiers ne seront pas analysés.

La section **Exceptions** permet d'exclure dossiers et fichiers qui ne doivent pas être analysés.

L'autorisation d'accès au menu d'analyse s'effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L'utilisateur peut procéder aux analyses antivirus**).

9.3. Analyse antivirale

L'analyse antivirale peut être utilisée pour vérifier l'ensemble de l'ordinateur ou des fichiers, des dossiers spécifiques à la recherche de malware. Si un virus est détecté, le client va automatiquement exécuter l'action définie dans **Paramètres**. Le ManagementServer sera notifié et un rapport sera ajouté au module **Évènements de sécurité** de G DATA Administrator.

Sélectionnez l'une des trois options suivantes et cliquez sur **Démarrer l'analyse antivirale** :

- **Analyser l'ordinateur entièrement** : vérifiera tous les fichiers et dossiers de l'ordinateur
- **Vérifier le secteur d'amorçage** : vérifiera le secteur d'amorçage (secteur boot)
- **Vérifier les fichiers et les dossiers** : vérifiera des fichiers et dossiers spécifiques. L'envergure peut être définie dans **Envergure de l'analyse**.

Sous **Paramètres**, les paramètres de l'analyse antivirale et les exceptions peuvent être configurées (voir **Gardien**).

Le module d'analyse antivirus peut être activé ou désactivé dans le G DATA Administrator sous **Paramètres du client** > **Généralités** > **Fonctions du client**.

9.4. Mise à jour

Le module Mise à jour s'assure que G DATA Security Client pour Mac dispose des dernières versions de signatures antivirales pour une protection optimale.

La date et l'heure de la dernière mise à jour des signatures s'affichent au niveau de **Dernière mise à jour**. La version exacte de chaque moteur s'affiche au niveau de **Moteur A** et **Moteur B**. Cliquez sur **Mise à jour des signatures antivirus** pour immédiatement lancer le processus de mise à jour.

Les paramètres des mises à jour de signatures antivirus sont disponibles dans **Paramètres** :

- **Source de la mise à jour des signatures** : définit si les clients doivent récupérer leurs mises à jour depuis le serveur ManagementServer local ou depuis les serveurs de mises à jour de G DATA sur internet (voir **Paramètres du client** > **Généralités** > **Mises à jour**).
- **Planification de la mise à jour** : définit la fréquence à laquelle doivent s'effectuer les mises à jour
- **Serveur Proxy** : paramétrages des informations pour accéder à internet via un serveur proxy si besoin
- **Données d'accès** : identifiants nécessaires pour pouvoir effectuer les mises à jour directement sur les serveurs G DATA sur internet

Les paramètres **Planification des mises à jour**, **Serveur Proxy** et **Données d'accès** ne sont utilisés que si **Charger les mises à jour antivirus depuis le ManagementServer** n'a pas été sélectionné sous **Source de la mise à jour des signatures** (voir **Paramètres du client** > **Généralités** > **Mises à jour**).

L'autorisation d'accès au menu Mises à jour des signatures antivirus s'effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L'utilisateur peut télécharger les mises à jour des signatures**).

9.5. Quarantaine

Le module quarantaine affiche les objets qui ont été placés en quarantaine par le **Gardien** ou par une **Analyse antivirus**.

Pour chaque objet les informations suivantes sont affichées :

- **Nom du fichier** : Le nom et l'emplacement de l'objet infecté.
- **Nom du virus** : Le nom du virus qui a infecté l'objet.
- **Taille fichier** : La taille fichier de l'objet.

Sélectionnez un ou plusieurs objet(s) puis cliquez sur un des boutons suivants :

- **Désinfecter et restaurer** : Retire le virus de l'objet puis le restaure à son emplacement original.
- **Restaurer** : Restaure l'objet à son emplacement original. Attention : si l'objet n'est pas d'abord désinfecté, il y a de forte chance qu'il infecte le système.
- **Supprimer** : Supprime l'objet de la quarantaine.

L’autorisation d’accès au menu **Quarantaine** s’effectue via G DATA Administrator **Paramètres du client** > **Généralités** > **Fonctions du client** (**L’utilisateur peut afficher la quarantaine locale**)

9.6. À propos de G DATA Security Client

La fenêtre A propos affiche le statut d’informations à propos de G DATA Security Client pour Mac :

- **Version** : La version du client installé
- **ManagementServer** : Le nom du ManagementServer auquel le client est rattaché.
- **Statut du logiciel de Sécurité** : Le statut des services d’arrière-plan du client.

10. G DATA ActionCenter

G DATA ActionCenter met à disposition certains services G DATA via le cloud. Ses fonctionnalités sont divisées en modules. Après avoir **créé un compte** et vous être connecté à son interface web via l'adresse **https://ac.gdata.de**, vous pourrez choisir un module, soit sur l'écran principal sous **Modules** soit via le **Menu** dans le coin supérieur droit:

- **Mes Appareils** : Mobile Device Management pour les versions pour particuliers de G DATA Internet Security pour Android.
- **Network Monitoring** : Surveille l'infrastructure réseau pour prévenir et fournir une réponse rapide en cas de panne.

Les raccourcis suivants sont listés sous **Paramètres** :

- **Autorisations** : Gérer les permissions pour les autres comptes ActionCenter comme les permissions lecture seule de **Network Monitoring**.
- **Groupes e-mail** : Configure les groupes d'e-mails pour l'envoi des rapports et notifications, tels que les alertes de **Network Monitoring**.

ActionCenter permet aussi la gestion des appareils iOS en effectuant le lien entre les appareils et G DATA ManagementServer. La configuration d'iOS Mobile Device Management s'effectue via le nœud **iOS Mobile Device Management** qui se trouve dans la fenêtre **Clients** de G DATA Administrator.

10.1. Créer et lier un compte

Sur la page de connexion de G DATA ActionCenter, cliquez sur **S'enregistrer** pour ouvrir la page d'enregistrement. Après avoir entré puis confirmé une **Adresse électronique** valide, saisir un **Mot de passe** de votre choix, cochez **J'accepte les conditions**, puis cliquez sur **S'enregistrer** pour finaliser la création du compte. Un e-mail contenant un lien de confirmation sera envoyé à l'adresse e-mail précédemment indiquée.

Après avoir cliqué sur le lien pour confirmer la création du compte, les identifiants ("nom d'utilisateur" / "mot de passe") doivent être saisis dans G DATA Administrator sous l'onglet **Serveur** > **ActionCenter**. Cette action établit la liaison entre G DATA ManagementServer et G DATA ActionCenter.

10.2. Modules

Les fonctionnalités de G DATA Action Center sont divisées en multiples modules. Pour les solutions Business, ActionCenter offre le module Network Monitoring.

10.2.1. Network Monitoring

Network Monitoring est un **module optionnel**.

Grace à Network Monitoring, les administrateurs supervisent l'état de leur infrastructure réseau. Par le paramétrage de **sondes**, une grande variété d'informations statistiques peut être collectée via les clients et consultée sur le Tableau de bord.

10.2.1.1. Tableau de bord

Le Tableau de bord affiche des statistiques, à jour, de toutes les **sondes**, ainsi qu'une vue d'ensemble de tous les **serveurs** et **appareils** pouvant être gérés. Lorsqu'une sonde est mise en favori, un Gadget récapitulatif contenant le nom des appareils associés, les dernières valeurs, et une courbe de tendance est ajouté au Tableau de bord.

Les informations sur l'état sont affichées au milieu du Tableau de bord. Les sondes n'ayant renvoyé aucune valeur déclencheur sont listées sous **OK**. Lorsqu'une sonde renvoie une valeur de déclenchement (inférieure ou supérieure aux valeurs seuils selon le paramétrage effectué), son statut passe à **Attentions**. Après deux autres dépassements des valeurs de déclenchement, elle est listée sous **Critique**. Lorsqu'elles sont triées par statut, les sondes sont affichées par catégories. Cela permet une vue d'ensemble granulaire de la catégorie d'appareils affectés.

La section **Journal** affiche les entrées au journal pour toutes les sondes. Des entrées sont consignées dans le journal lorsqu'une sonde envoie sa première valeur, lorsqu'elle fait remonter une erreur et lorsqu'elle change d'état (Par exemple elle passe de **OK** à **Critique**). Cliquer sur une entrée du journal ouvre la page de la **Sonde** associée.

En administrant plusieurs serveurs, le menu déroulant en haut du tableau de bord peut être utilisé pour créer et sélectionner des vues de tableau de bord. Cliquez sur **Créer un tableau de bord**, entrez un **Nom** pour le tableau de bord et assignez un ou plusieurs ManagementServer.

10.2.1.2. Vue d'ensemble des sondes

Une sonde est créée en attribuant un **modèle de sonde** à un ou plusieurs appareils. En fonction des paramètres du modèle de sonde, la sonde fera remonter régulièrement les rapports statistiques concernés depuis les appareils concernés. Cliquer sur **Créer sondes** pour **créer une nouvelle sonde**.

La page Vue d'ensemble des sondes liste toutes les sondes. Cliquer sur une sonde ouvre la page de la **Sonde** associée. La liste de sondes peut être triée par état ou par catégorie. Pour chaque entrée de la liste, les informations suivantes sont affichées :

- **ManagementServer** : Le ManagementServer gérant l'appareil auquel a été attribué le modèle de sonde.
- **Appareil** : L'appareil auquel a été attribué le modèle de sonde.
- **État** : L'état actuel de la sonde (**OK**, **Attention**, **Critique** or **Inconnue**).
- **Sonde** : Le nom du modèle de sonde qui a été utilisé pour créer la sonde.
- **Catégorie** : La catégorie du modèle de sonde qui a été utilisé pour créer la sonde.
- **Cible** : L'appareil cible du modèle de sonde qui a été utilisé pour créer la sonde.

Ajouter sondes

Créer une sonde implique l'attribution d'une ou plusieurs **modèles de sonde** à un ou plusieurs appareils. La page Ajouter sondes propose une configuration en quatre étapes :

1. **Choisir modèle(s) de sonde**. Choisir un ou plusieurs modèles. Les modèles sont listés par catégorie.
2. **Choisir appareil(s)**. Choisir un ou plusieurs appareils. Les appareils sont affichés dans une arborescence dossiers, eux-mêmes regroupés par ManagementServer. À la racine de l'arborescence, les ManagementServers eux-mêmes peuvent être sélectionnés (dans l'éventualité qu'à l'étape 1, un modèle de sonde ait été choisi dans la catégorie

ManagementServer).

3. **Vérifier les appareils sélectionnés**. S'assurer que tous les appareils auxquels les modèles doivent s'appliquer ont été sélectionnés.
4. **Rappel**. Cliquer sur **Créer une sonde** pour créer la sonde correspondante et revenir à la page **Vue d'ensemble des sondes**.

Sonde

La page de Sonde affiche les détails de la sonde sélectionnée. En haut de page sont affichés : **Nom**, **Appareils**, **ManagementServer** et statut actuel. En utilisant l'option **Favori**, la sonde peut être épinglée au **Tableau de bord**.

La vue diagramme peut être personnalisée pour avoir instantanément une vue d'ensemble des tendances. Les paramètres par défaut affichent les valeurs des 6 dernières heures. La fréquence peut être ajustée grâce au menu déroulant.

Plusieurs paramètres sont affichés sous **Vue d'ensemble**:

- **Intervalle de mesure** : L'intervalle auquel la sonde envoie de nouvelles valeurs à ActionCenter.
- **Dernière valeur** : La valeur la plus récente accompagnée de l'horodatage.
- **Minimum** : la valeur la plus basse jamais enregistrée.
- **Maximum** : La valeur la plus élevée jamais enregistrée.
- **Déclencheur** (ne s'affiche que si un déclencheur a été configuré) : Valeur actuelle du déclencheur.
- **Au-dessus déclencheur** (ne s'affiche que si un déclencheur a été configuré) : Le pourcentage de valeurs enregistrées, supérieures à la valeur de déclenchement.
- **En dessous déclencheur** (ne s'affiche que si un déclencheur a été configuré) : Le pourcentage de valeurs enregistrées, inférieures à la valeur de déclenchement.

Sous **Journal de sonde** sont consignées toutes les entrées journal pour cette sonde. Des entrées sont consignées dans le journal lorsqu'une sonde envoie sa première valeur, lorsqu'elle fait remonter une erreur et lorsqu'elle change d'état (Par exemple elle passe de **OK** à **Critique**).

Gérer les modèles de sonde

Un modèle de sonde contient les paramètres pour un scénario spécifique de surveillance réseau. Les modèles peuvent être attribués à un ou plusieurs appareils, créant par la même des **sondes**.

La page Gérer les modèles de sonde liste tous les modèles de sonde. Pour chaque entrée de la liste, les informations suivantes sont affichées :

- **Nom** : Le nom du modèle.
- **Commentaire** : Un descriptif du modèle permettant ainsi de les distinguer les uns des autres.
- **Catégorie** : La catégorie du modèle (**Appareils**, **Processus local**, **Réseau**, **ManagementServer**, **Imprimante réseau** ou **Appareils SNMP**).
- **Sondes** : En fonction de la Catégorie sélectionnée, le type d'informations surveillées est défini.
- **Utilisé par** : Indique le nombre d'appareils auxquels a été attribué une **sonde** utilisant ce modèle.

Cliquer sur un modèle dans la liste pour ouvrir la page **Éditer un modèle**. Cliquer sur **Créer un**

modèle pour créer un nouveau modèle de sonde.

Créer un modèle

Un certain nombre de paramètres, obligatoires et optionnels, doivent être saisis pour créer un modèle de sonde.

- **Catégorie** : Choisi la catégorie du modèle (**Appareils**, **Processus local**, **Réseau**, **ManagementServer**, **Imprimante** ou **Appareils SNMP**).
- **Sonde** : En fonction de la **Catégorie** sélectionné, le type d'informations surveillées est défini.
- **Nom** : Le nom du modèle.
- **Commentaire** : Un descriptif du modèle permettant ainsi de les distinguer les uns des autres.

En fonction de la **Catégorie** et de la **Sonde**, un ou plusieurs des paramètres suivant seront affichés:

- **Cible** : Cible sur laquelle les informations sélectionnées vont être collectées. Cette valeur ne peut pas être changée et est configurée par défaut sur *localhost*. Ceci signifie que les informations seront collectées sur l'appareil sur lequel le modèle de sonde sera attribué.
- **Nom d'hôte** : Le nom d'hôte de l'appareil sur lequel les informations choisies vont être surveillées. Il n'est pas nécessaire que ce soit l'appareil auquel va être attribué le modèle de sonde. Plusieurs noms d'hôtes peuvent être ajoutés; lorsque le modèle de sonde est attribué à un appareil, plusieurs sondes seront créées.
- **URL** : l'URL pour laquelle les informations sélectionnées vont être surveillées. Plusieurs URLs peuvent être ajoutées; lorsque le modèle de sonde est attribué à un appareil, plusieurs sondes seront créées.
- **Instance SQL Serveur** : L'instance de serveur SQL pour laquelle les informations sélectionnées seront surveillées. Cliquez sur la loupe pour voir une liste des instances de serveur SQL disponibles, par ManagementServer.

Les paramètres optionnels aussi dépendent de la **Catégorie** et de la **Sonde** sélectionnée, et incluent un ou plusieurs des éléments suivants :

- **Valeur seuil** : Configure une valeur seuil.
- **Condition de valeur mesurée** : Détermine comment la valeur seuil est interprétée. La valeur de la sonde va changer de **OK** vers **Attention** puis vers **Critique** lorsque les valeurs mesurées sont en dessous ou au-dessus des valeurs seuil.
- **Processeur** : Saisir le processeur pour lequel les informations sélectionnées vont être surveillées ou saisir *_Total* pour surveiller tous les processeurs.
- **Lettre de lecteur** : Saisir le lecteur pour lequel les informations sélectionnées vont être surveillées ou saisir *_Total* pour surveiller tous les lecteurs.
- **Nom du processus** : Le processus pour lequel les informations sélectionnées seront surveillées ou entrez *_Total* pour surveiller tous les processus.
- **Nom du périphérique réseau** : Saisir le périphérique réseau pour lequel les informations sélectionnées vont être surveillées ou saisir * pour surveiller tous les périphériques réseau.
- **Base de données SQL Serveur** : Saisir la base de données pour laquelle les informations sélectionnées vont être surveillées ou saisir *_Total* pour surveiller toutes les base de données.
- **Délai de réponse** : Saisir le délai de réponse pour les requêtes Ping.
- **Code HTTP de statut attendu** : Lorsque la requête HTTP renvoie un code HTTP de statut

différent de celui défini ici, ceci est considéré comme une violation de la valeur seuil, et change donc l'état de la sonde.

- **SNMP Community** : saisir la chaine de caractère SNMP Community nécessaire par l'appareil cible. La chaine de caractère Community est configurée par le fabriquant de l'appareil et souvent peut être trouvée dans la documentation de l'appareil.

Dans **Configuration des Alertes**, Les alertes e-mails peuvent être paramétrées.

- **Condition d'alerte** : Une alerte sera envoyée seulement lorsque l'état de la sonde change pour **Critique** ou lorsqu'il change soit pour **Critique**, soit pour **Attention**.
- **Prévenir uniquement les groupes e-mail sélectionnés** : L'alerte sera envoyée aux groupes e-mail sélectionnés, ceux-ci peuvent être définis en utilisant les **Groupes e-mail**.

Modifier un modèle
La page Modifier un modèle peut être utilisée pour modifier des modèles de sonde déjà existants. Tous les paramètres correspondent à ceux ayant été définis lorsque le modèle a été créé. Certains sont affichés comme lecture-seule et ne peuvent pas être modifiés :

- **Catégorie**
- **Sonde**
- **Utilisé par**
- **Cible**
- **Nom d'hôte**
- **URL**

Tous les autres paramètres peuvent être librement modifiés. Cliquer sur **Enregistrer le modèle** pour enregistrer les modifications. Les modifications effectuées sur un modèle existant seront appliquées à toutes les sondes basées sur le modèle sélectionné.

10.2.1.3. Vue d'ensemble serveur

La vue d'ensemble serveur affiche tous les ManagementServers qui ont été reliés au compte ActionCenter. Par serveur, la vue liste le nombre d'**appareils** , de **sondes** et d'imprimantes associés. La vue d'ensemble peut être triée en cliquant sur les tags sous **Trier**.

Cliquer sur un serveur ouvre la page **Information serveur**, ce qui donne accès aux informations et paramètres suivants :

- **Nom d'hôte** : Le nom d'hôte du serveur.
- **Version** : Le numéro de version du ManagementServer.
- **Dernier accès** : L'horodatage de la dernière synchronisation entre ce serveur et ActionCenter.
- **Sonde** : Le nombre de sondes associées à ce serveur.
- **Appareils** : Le nombre d'appareils associés à ce serveur.
- **Imprimantes** : Le nombre d'imprimantes associées à ce serveur.
- **Commentaire** : Un descriptif du serveur permettant ainsi de les distinguer les uns des autres.
- **Accès API** : Activé par défaut. Désactiver l'accès API ne supprime pas le serveur dans l'ActionCenter mais l'empêche d'envoyer des valeurs.

- **Tags** : Ajoute un ou plusieurs tags qui pourront être utilisés pour effectuer des tris dans la liste Vue d'ensemble serveur.

Cliquez sur **Définir des autorisations** pour autoriser un autre compte ActionCenter à accéder à ce serveur en lecture-seule. Dans le champ **Adresse e-mail**, saisissez l'adresse e-mail du compte puis cliquez sur **Envoyer l'invitation** pour envoyer un e-mail d'invitation. Le destinataire aura accès, en lecture-seule, à toutes les fonctions d'administration du réseau de ce serveur après s'être connecté et avoir accepté l'invitation sur l'ActionCenter via le lien. Les permissions peuvent être consultées et révoquées via la page **Autorisation**.

> Si l'addresse e-mail n'est associée à aucun compte ActionCenter, le destinataire sera invité à créer un compte avant de pouvoir accepter l'invitation.

Cliquer sur **Supprimer serveur** pour supprimer ce serveur de ActionCenter. Par la même occasion, ceci supprimera tous les **appareils**, **sondes** et journaux associés.

10.2.1.4. Vue d'ensemble appareils

La vue d'ensemble appareils liste tous les appareils gérés par les ManagementServers qui ont été liés au compte ActionCenter. La liste peut être triée en cliquant sur **Trier** et en sélectionnant le ManagementServer approprié depuis l'arborescence.

Chaque appareil est listé avec son nom et les sondes qui lui sont associées. Cliquer sur une sonde ouvre la page de la **Sonde** associée.

10.3. Paramètres

La section Paramètres contient les paramètres qui peuvent être utilisés par d'autres modules ActionCenter.

10.3.1. Autorisations

La page d'autorisations peut être utilisée pour gérer les autorisations allouées sous **Network Monitoring** > **Vue d'ensemble serveur**. Les comptes ActionCenter avec des autorisations sont listés sous la dénomination des ManagementServer respectifs. Cliquez sur **Supprimer** pour annuler la permission du compte sélectionné.

10.3.2. Groupes d'email

Les groupes d'e-mails regroupent une ou plusieurs adresses e-mail et sont utilisés pour les rapports et notifications, tel que les alertes de seuil du module **Network Monitoring**. La page Groupes e-mails affiche tous les groupes e-mail ainsi que les adresses e-mails qui leur sont associées.

Pour créer un nouveau groupe e-mail, cliquer sur **Ajouter un groupe e-mail**, saisir un **Nom**, sélectionner la **Langue** désirée puis cliquer sur **Ajouter**. Pour ajouter une adresse e-mail à une groupe, sélectionner le groupe puis, dans la section **Modifier groupe "nom du groupe"**, saisir une **Adresse e-mail** puis cliquer sur **Ajouter e-mail à "nom du groupe"** . Cette étape peut être répétée autant de fois que nécessaire pour ajouter d'autre adresses e-mail à un groupe.

11. G DATA MailSecurity MailGateway

G DATA MailSecurity est un **module optionnel**.

G DATA MailSecurity MailGateway permet d'assurer la protection complète de vos communications par courrier électronique. Parallèlement au logiciel exécuté en arrière-plan, l'application **MailSecurity Administrator**, qui vous permet d'accéder à l'ensemble des fonctions et options de l'application MailGateway, est automatiquement installée. Lors d'une installation standard, ce programme est disponible sous **Démarrer** > **Programmes** > **G DATA MailSecurity** > **G DATA MailSecurity**. Lorsque vous quittez le logiciel Administrator, l'application MailGateway reste ouverte. Elle reste activée en arrière-plan et gère les processus définis.

Vous pouvez également assurer la maintenance de l'application MailGateway à partir des ordinateurs qui répondent à la configuration système requise pour l'outil administrateur G DATA MailSecurity. Si vous souhaitez contrôler MailGateway à partir d'un autre ordinateur du réseau, il vous suffit d'installer le programme Administrator sans le logiciel MailGateway. Redémarrez alors le programme d'installation et sélectionnez le bouton **G DATA MailSecurity Administrator**.

12. G DATA MailSecurity Administrator

G DATA MailSecurity est un **module optionnel**.

Le logiciel G DATA MailSecurity Administrator est le logiciel de commande de G DATA MailSecurity MailGateway. Il sécurise l'ensemble du trafic de courriers électroniques SMTP et POP3 du réseau. De plus, il est géré de manière centralisée par l'administrateur système. L'application Administrator peut être démarrée avec un mot de passe à partir d'un ordinateur Windows. Toutes les modifications des paramètres du scanner antivirus et des mises à jour des signatures antivirus peuvent être effectuées en tant que tâches à distance.

12.1. Lancement de l'application G DATA MailSecurity Administrator

L'outil d'administration permet de gérer la passerelle de messagerie, il est disponible sous **G DATA MailSecurity** dans le groupe de programmes **Démarrer** > **Tous les programmes** ou **Programmes** > **G DATA MailSecurity** du menu Démarrer. Lors du démarrage de l'outil d'administration, vous êtes invité à indiquer le serveur et le mot de passe. Dans le champ **Serveur**, saisissez le nom ou l'adresse IP de l'ordinateur sur lequel est installée la passerelle de messagerie.

Aucun **Mot de passe** n'est défini lors de la première connexion. Cliquez sur le bouton **OK** sans saisir de mot de passe. Une fenêtre de saisie du mot de passe, dans laquelle vous devez saisir un nouveau mot de passe pour G DATA MailSecurity Administrator sous **Nouveau mot de passe**, s'affiche. Confirmez le mot de passe saisi en le saisissant de nouveau dans le champ **Confirmer le nouveau mot de passe** et en cliquant ensuite sur **OK**. Vous pouvez à tout moment modifier le mot de passe dans la rubrique **Options** de l'onglet **Avancé** en cliquant sur le bouton **Modifier le code**.

12.2. Configurer l'application G DATA MailSecurity Administrator

La barre de menus de l'application G DATA MailSecurity Administrator contient les options suivantes :

- **Options** : vous pouvez modifier ici les paramètres de base de l'application G DATA MailSecurity et les adapter à vos besoins.
- **Mise à jour** : dans la rubrique Mise à jour Internet, vous pouvez définir les paramètres de base pour le téléchargement automatique des signatures antivirus depuis Internet. Vous pouvez ainsi adapter la planification des téléchargements à vos besoins et procéder à la mise à jour des fichiers du programme G DATA MailSecurity.
- **Filtre antispam** : l'icône Filtre antispam propose un raccourci vers les paramètres **Filtre Antispam** du module **Filtre**.
- **Aide** : ici vous pouvez accéder à l'aide en ligne du programme.
- **Infos** : ici vous obtenez des informations sur la version du programme.

12.2.1. Options

La rubrique Options vous permet de définir une multitude de paramètres grâce auxquels vous pouvez adapter G DATA MailSecurity de manière optimale aux conditions de votre réseau. Pour ce faire, différentes rubriques de paramétrage thématiques, sous différents onglets, sont mises à votre disposition. Pour les afficher, cliquez sur les onglets correspondants.

12.2.1.1. Entrant (SMTP)

Cette rubrique vous offre la possibilité de définir tous les paramètres nécessaires à l'analyse antivirus des courriers SMTP entrants au niveau de votre serveur de messagerie.

Réception

Cette option permet de traiter ou non les courriers entrants. Le port 25 est paramétré par défaut. Si, en raison de circonstances particulières, ce port standard n'est pas utilisé, vous pouvez définir, à l'aide du bouton **Configurer**, d'autres paramètres pour le port et le protocole des courriers entrants.

Transfert

Dans le cadre du transfert des courriers entrants à votre serveur de messagerie, désactivez l'option **Utiliser le serveur DNS pour l'envoi du courrier** et indiquez le serveur souhaité sous **Transmettre les courriers au serveur SMTP suivant**. Indiquez également le **Port** par le biais duquel les courriers doivent être transmis au serveur SMTP. Si plusieurs cartes réseau sont à votre disposition, vous pouvez sélectionner laquelle utiliser sous **Adresse IP d'expédition**.

Protection du relais

Pour éviter toute utilisation abusive de votre serveur de messagerie, vous pouvez et devez définir, sous **Accepter uniquement les courriers entrants pour les domaines suivants ou les adresses suivantes**, les domaines auxquels les courriers SMTP peuvent être envoyés. Votre serveur ne peut ainsi pas être utilisé pour la transmission de spam vers d'autres domaines.

> **Attention** : si aucun domaine n'est saisi ici, aucun courrier électronique n'est accepté. Si vous souhaitez accepter les courriers électroniques de tous les domaines, vous devez ajouter ici *.* (astérisque point astérisque).

La protection du relais peut également être assurée à l'aide d'une liste d'adresses électroniques valides. Les courriers pour les destinataires qui ne figurent pas dans cette liste ne sont pas acceptés. Pour automatiser l'actualisation des adresses électroniques, celles-ci peuvent être lues automatiquement et régulièrement à partir de **Active Directory**. L'application .NET Framework 1.1 (ou une version supérieure) est nécessaire à la connexion Active Directory.

12.2.1.2. Sortant (SMTP)

Cette rubrique vous offre la possibilité de définir tous les paramètres nécessaires à l'analyse antivirus des courriers SMTP sortants au niveau de votre serveur de messagerie.

Réception

La case à cocher **Traiter le courrier sortant** vous permet de définir si vous souhaitez contrôler l'absence de virus dans les courriers SMTP sortants. Sous **Adresses IP/sous-réseaux des ordinateurs qui envoient les courriers sortants**, vous pouvez définir les adresses IP d'où proviennent les courriers à vérifier. S'il est question de plusieurs adresses IP, séparez les différentes adresses à l'aide d'une virgule. Cette saisie est nécessaire pour permettre à la passerelle de distinguer les courriers entrants des courriers sortants. Le port 25 est paramétré par défaut pour la réception des courriers sortants. Si, en raison de circonstances particulières, ce port standard n'est pas utilisé, vous pouvez définir, à l'aide du bouton **Configurer**, d'autres paramètres pour les courriers sortants.

Transfert

Activez l'option **Utiliser le serveur DNS pour l'envoi du courrier** pour envoyer les courriers via le serveur de messagerie compétent du domaine cible. Si vous souhaitez envoyer les courriers par l'intermédiaire d'un relais (un fournisseur, par exemple), désactivez l'option Utiliser le serveur DNS

pour l'envoi du courrier et définissez le relais sous **Transmettre les courriers au serveur SMTP suivant**. Si plusieurs cartes réseau sont à votre disposition, vous devez sélectionner laquelle utiliser sous **Adresse IP d'expédition**.

12.2.1.3. Entrant (POP3)

Cette rubrique vous offre la possibilité de définir tous les paramètres nécessaires à l'analyse antivirus des courriers POP3 entrants au niveau de votre serveur de messagerie.

Demandes

Sous **Traiter les demandes POP3**, vous avez la possibilité d'utiliser G DATA MailSecurity pour récupérer les courriers POP3 à partir du serveur POP3 correspondant, de les soumettre à une analyse antivirus et de les transmettre aux destinataires par le biais du serveur de messagerie. Vous devez éventuellement indiquer le **Port** utilisé par votre programme de messagerie pour les demandes POP3 (généralement le port 110). La fonction **Éviter le dépassement de temps au niveau du programme de messagerie** vous permet de pallier à la durée requise par G DATA MailSecurity pour vérifier les courriers électroniques et d'éviter que le destinataire ne reçoive une erreur d'expiration à la récupération des courriers POP3 à partir de son programme de messagerie, par exemple, car les données ne sont pas immédiatement disponibles (au lieu de cela, le transfert du message est retardé de quelques secondes).

Les programmes de messagerie POP3 peuvent être configurés manuellement. Pour ce faire, dans votre programme de messagerie, utilisez 127.0.0.1 ou le serveur de votre passerelle de messagerie comme serveur POP3 entrant et saisissez le nom du serveur de messagerie externe et le nom de l'utilisateur en les séparant par un signe deux-points. Ainsi, au lieu de *serveur POP3:mail.xxx.fr/nom d'utilisateur:Sophie Martin*, saisissez *serveur POP3:127.0.0.1/nom d'utilisateur:mail.xxx.fr:Sophie Martin*. Pour procéder à une configuration manuelle, veuillez également vous reporter au manuel d'utilisation du programme de messagerie pour connaître les étapes nécessaires.

Répétition

Sous **Collecter les courriers du serveur POP3 suivant**, vous devez indiquer le serveur POP3 à partir duquel vous souhaitez collecter le courrier (*pop3.fournisseur de services de messagerie.fr*, par exemple).

Filtre

Si des courriers POP3 sont refusés suite à une vérification du contenu ou une attaque de virus, l'expéditeur du message peut en être automatiquement informé. Le texte de remplacement des courriers refusés est le suivant : *Le message a été refusé par l'administrateur système*. Vous pouvez toutefois paramétrer cette fonctionnalité d'avertissement. Vous pouvez également utiliser des caractères génériques, qui correspondent à des données relatives au message refusé dans le texte de notification. Pour le texte que vous pouvez librement définir au niveau de l'**Objet** et du **Corps du courrier**, vous pouvez utiliser les caractères génériques suivants (un signe de pourcentage suivi d'une minuscule) :

- %v > Virus
- %s > Expéditeur
- %r > Destinataire
- %c > Cc
- %d > Date
- %u > Objet

- %h > En-tête
- %i > Adresse IP de l'expéditeur

12.2.1.4. Analyse antivirus

Lors de l'analyse antivirus, vous avez la possibilité de définir les options d'analyse pour les courriers entrants et sortants.

Entrant
Vous devez bien évidemment avoir activé la fonction **S'assurer de l'absence de virus dans les courriers entrants** et identifier l'option **En cas de contamination** que vous souhaitez utiliser.

- **Uniquement enregistrer l'événement**
- **Désinfecter (si impossible : uniquement enregistrer l'événement)**
- **Désinfecter (si cela n'est pas possible : renommer)**
- **Désinfecter (si impossible : supprimer le fichier)**
- **Renommer les pièces jointes infectées**
- **Supprimer les pièces jointes infectées**
- **Supprimer le message**

N'utilisez l'option **Uniquement enregistrer l'événement** que si votre système est protégé en permanence d'une autre manière contre les attaques de virus (par exemple, en utilisant G DATA Antivirus Business).

Lorsque des virus sont détectés, vous disposez d'un grand nombre d'options de notification. Vous pouvez ainsi insérer un avertissement virus dans l'objet et le corps du texte du courrier infecté, de manière à informer le destinataire. Vous pouvez également envoyer un message relatif au virus détecté à certaines personnes, au gestionnaire du système ou aux collaborateurs compétents, par exemple, afin de les informer qu'un virus a été envoyé à une adresse électronique de leur réseau. Si vous saisissez plusieurs adresses de destinataires, séparez-les par un point-virgule.

Vous pouvez personnaliser le texte des notifications. Vous pouvez utiliser ici les mêmes caractères génériques que dans la rubrique **Entrant (POP3)** > **Filtre**.

Sortant
Activez la fonction **S'assurer de l'absence de virus dans les courriers sortants** et sélectionnez par défaut **Ne pas envoyer le message infecté**. De cette manière, aucun virus ne quitte votre réseau et ne peut occasionner de dommages chez vos partenaires commerciaux. En cas d'infections, un grand nombre d'options de notification vous sont proposées. Vous pouvez ainsi **Informer l'expéditeur de l'infection du message** et, grâce à l'option **Envoyer un message de Virus aux personnes suivantes**, notifier au gestionnaire du système ou aux collaborateurs compétents, par exemple, qu'un virus a été détecté sur votre réseau. Si vous saisissez plusieurs adresses de destinataires, veuillez les séparer par un point-virgule.

Vous pouvez organiser individuellement le texte des fonctions de notification. Il vous suffit de cliquer sur le bouton **...** de droite. Vous pouvez utiliser ici les mêmes caractères génériques que dans la rubrique **Entrant (POP3)** > **Filtre**.

L'option **Joindre un compte-rendu aux courriers sortants (non infectés)** vous offre la possibilité d'ajouter, à la fin du texte des messages vérifiés à l'aide de l'application G DATA MailSecurity, un

message indiquant clairement que le courrier a été vérifié à l'aide de G DATA MailSecurity. Vous pouvez bien évidemment également modifier ou supprimer ce rapport.

G DATA ManagementServer
Si MailGateway est installé sur un ordinateur protégé par une solution professionnelle de G DATA (AntiVirus Business, Client Security Business ou Endpoint Protection Business), vous pouvez activer l'option **Envoyer un message de détection de virus à G DATA ManagementServer** et ainsi profiter de l'infrastructure client/serveur pour avoir une remonter cohérente des tentatives d'infection détectées.

12.2.1.5. Paramètres d'analyse

Cette rubrique vous permet d'optimiser les performances de détection des virus de l'application G DATA MailSecurity et de les adapter à vos besoins personnels. De manière générale, diminuer les performances de détection de virus permet d'augmenter les performances du système tandis qu'augmenter des performances de détection de virus peut entraîner une légère baisse des performances. La situation varie au cas par cas.

Différentes fonctions sont disponibles à partir des boutons suivants :

- **Utiliser les moteurs** : G DATA MailSecurity fonctionne avec deux moteurs antivirus, qui opèrent indépendamment l'un de l'autre. Définissez ici comment les deux moteurs doivent coopérer. L'utilisation des deux moteurs garantit des résultats optimaux pour la détection des virus. En revanche, l'utilisation d'un seul moteur comporte certains avantages de performances, car le processus d'analyse est plus rapide.
- **Types de fichiers** : vous pouvez définir ici quels Types de fichiers seront analysés par G DATA MailSecurity. Nous vous conseillons ici l'option Détection automatique du type de fichier qui ne vérifie automatiquement que les fichiers théoriquement susceptibles de contenir un virus. Si vous souhaitez définir vous-même les types de fichiers qui doivent être soumis à une analyse antivirus, utilisez la fonction **Défini par l'utilisateur**. Cliquez sur le bouton **...** pour ouvrir une boîte de dialogue dans laquelle vous pouvez saisir les types de fichiers souhaités dans la zone de saisie supérieure, puis les ajouter à la liste des types de fichiers définis par l'utilisateur à l'aide du bouton **Ajouter**. Vous pouvez également travailler avec des caractères génériques.

  Le point d'interrogation (?) remplace des caractères individuels. L'astérisque (*) remplace des suites de caractères. Par exemple, pour vérifier l'intégralité des fichiers comportant l'extension de fichier exe, vous devez saisir **.exe*. Pour vérifier les fichiers de feuilles de calcul de différents formats (.xlr, .xls, par exemple), il vous suffit de saisir **.xl?*. Pour vérifier les fichiers de différents types mais portant un début de nom similaire, saisissez *text*.**.
- **Heuristique** : lorsque l'analyse heuristique est utilisée, les virus sont reconnus non seulement par le biais de la base de données des virus actualisée en permanence, mais également au moyen de certaines caractéristiques typiques aux virus. Cette méthode augmente le niveau de sécurité, mais de fausses alertes peuvent être déclenchées dans de rares cas.
- **Analyser les archives** : l'analyse des fichiers compressés des archives doit généralement être activée.
- **OutbreakShield** : la technologie OutbreakShield permet de détecter et de combattre les programmes malveillants dans les envois massifs de messages électroniques avant que les signatures antivirus correspondantes ne soient disponibles. Cette technologie surveille le trafic mondial de courriers électroniques et identifie les pics d'envoi de courriers suspects. Selon une multitude de critères, les courriers dangereux sont identifiés et bloqués ce qui lui permet de

combler quasiment en temps réel le laps de temps entre le début d'un envoi massif de messages électroniques infectés et son traitement au moyen de signatures adaptées. Si vous souhaitez utiliser OutbreakShield, utilisez le bouton **Paramètres** pour indiquer si vous utilisez un serveur proxy et, pour assurer à OutbreakShield un accès permanent à Internet, saisissez les **Codes d'accès pour la connexion à Internet**. Au niveau de l'onglet OutbreakShield, vous pouvez définir le texte du message que reçoit le destinataire du courrier si du spam qui lui était destiné a été refusé.

En raison de son architecture autonome, la technologie OutbreakShield ne peut ni désinfecter, ni renommer ou placer en quarantaine les pièces jointes infectées. Le texte de remplacement informe donc l'utilisateur que le courrier suspecté ou infecté ne peut lui être remis. Aucun message n'est émis au sujet des courriers refusés par OutbreakShield lorsque vous sélectionnez l'option **Supprimer le message**, sous **En cas d'infection**, dans l'onglet **Analyse antivirus** > **Entrant**. Tous les courriers infectés, y compris ceux exclusivement détectés par OutbreakShield, sont alors directement supprimés.

- **Protection anti-hameçonnage** : activez la protection anti-hameçonnage pour bloquer les courriers électroniques qui tentent d'obtenir des mots de passe, des informations relatives aux cartes de crédit et autres données personnelles en se faisant passer pour des courriers électroniques provenant d'établissements sérieux.

12.2.1.6. File d'attente

Cette rubrique vous permet de définir quand et à quel intervalle l'envoi des courriers électroniques non transmis par la passerelle au serveur de messagerie correspondant doit avoir lieu.

Les courriers électroniques sont généralement placés dans la file d'attente après l'analyse antivirus par G DATA MailSecurity. Les courriers peuvent être placés dans la file d'attente pour différentes raisons. Par exemple, le serveur de messagerie auquel les courriers doivent être transmis après analyse antivirus peut être surchargé ou en panne.

Messages ne pouvant être distribués

Sous **Intervalle de répétition**, indiquez l'intervalle à l'issue duquel G DATA MailSecurity doit procéder à une nouvelle tentative d'envoi. Ainsi, la saisie *1, 1, 1, 4*, indique que G DATA MailSecurity tente d'envoyer le courrier toutes les heures pendant les trois premières heures, puis régulièrement, toutes les quatre heures. Sous **Durée d'attente de l'erreur**, vous décidez quand l'envoi du courrier électronique doit être définitivement annulé et le courrier électronique supprimé.

Vous pouvez **Notifier l'expéditeur de messages dans la file d'attente toutes les ... heures** (la valeur ...doit être une heure entière). Si vous ne souhaitez pas informer régulièrement l'expéditeur de la non-distribution d'un message, il vous suffit de saisir *0* ici. Même si vous désactivez cette notification, les expéditeurs sont informés lorsque la distribution des courriers électroniques est définitivement annulée et que les courriers électroniques sont supprimés du serveur.

Le bouton **Rétablir les valeurs standards** vous permet de rétablir les paramètres standards de la rubrique File d'attente. Ces paramètres ont fait leurs preuves dans la pratique.

Limitation de la taille

Vous pouvez limiter la taille de la file d'attente à votre guise. Ceci sert à protéger des attaques de type Déni de Service. Une fois la taille atteinte, plus aucun nouveau courrier n'est ajouté à la file d'attente.

12.2.1.7. Avancé

La rubrique Avancé vous permet de modifier les paramètres globaux de G DATA MailSecurity.

Bannière SMTP

Le champ **Domaine** affiche par défaut le nom de l'ordinateur. Lors de l'envoi de courriers via le serveur DNS, vous devez saisir le nom de domaine complet ici pour permettre les recherches inversées. Activez l'option **Afficher uniquement le domaine** pour empêcher l'affichage de la version du serveur lors de la communication avec d'autres serveurs.

Limitation

Pour limiter le nombre de connexions SMTP traitées simultanément par G DATA MailSecurity, cochez la case **Limiter le nombre de connexions client SMTP**. G DATA MailSecurity autorise alors uniquement le nombre maximal de connexions indiqué. Vous pouvez ainsi adapter le filtrage des messages à la capacité du matériel utilisé pour la passerelle de messagerie.

Messages du système

L'**Adresse de l'expéditeur pour les messages du système** est l'adresse électronique utilisée pour informer l'expéditeur et le destinataire de la présence de virus dans les courriers ou de l'ajout de leurs courriers à la file d'attente. Les avertissements du système G DATA MailSecurity ne dépendent pas de la communication générale dans le cadre de la détection de virus. Les avertissements du système sont généralement des informations plus globales, sans rapport avec un courrier potentiellement infecté. G DATA MailSecurity envoie ainsi un avertissement du système lorsque le contrôle antivirus n'est plus garanti pour une raison quelconque.

Paramètres

Les boutons **Importer** et **Exporter** permettent d'enregistrer les paramètres des options de programme en tant que fichier XML pour de nouveau y avoir accès si besoin.

Modifier le code

Vous pouvez modifier ici le mot de passe administrateur indiqué au premier démarrage de G DATA MailSecurity. Pour ce faire, il vous suffit de saisir le mot de passe actuel sous **Ancien code** et le nouveau mot de passe sous **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. La modification du mot de passe est effectuée lorsque vous cliquez sur le bouton **OK**.

12.2.1.8. Journalisation

La rubrique Journalisation vous permet d'analyser de manière statistique les courriers électroniques entrants et sortants sur votre serveur. Les résultats statistiques peuvent être affichés dans la rubrique **Statistiques** de l'interface du programme. Pour ce faire, cliquez sur le bouton **Statistiques** de la rubrique **État** du programme. Vous pouvez également enregistrer les journaux dans un fichier externe (maillog.txt, situé dans le dossier d'installation de MailSecurity). Les fonctions **Uniquement spams** et **Limiter le nombre d'e-mails** vous permettent de limiter la taille de ce fichier journal si nécessaire.

12.2.2. Mise à jour

La rubrique Mise à jour vous permet de définir une multitude de paramètres grâce auxquels vous pouvez adapter G DATA MailSecurity en fonction de votre réseau. Vous pouvez choisir la manière dont les signatures antivirus et les fichiers du programme G DATA MailSecurity sont mises à jour.

12.2.2.1. Paramètres

Vous pouvez définir ici les paramètres de base de la mise à jour Internet. Si vous utilisez (par exemple, dans le cadre de la solution G DATA AntiVirus Business), parallèlement à l'application G DATA MailSecurity, le programme client/serveur G DATA AntiVirus, vous pouvez, grâce à l'option **Utiliser les signatures antivirus de l'application G DATA Security Client**, éviter de télécharger deux fois les signatures antivirus et utiliser directement les signatures de l'application G DATA Security Client installée. L'option **Procéder manuellement à la mise à jour Internet des signatures de virus** permet de planifier cette procédure pour une mise à jour via Internet. Le bouton **Paramètres et planification** donne accès à l'ensemble des paramètres de planification nécessaires aux mises à jour Internet manuelles et automatiques.

Codes d'accès

Sous Codes d'accès, saisissez le **Nom d'utilisateur** et le **Mot de passe** que vous avez reçus lors de l'enregistrement de votre licence G DATA MailSecurity. Le serveur G DATA les utilisera pour vous authentifier et lors de la mise à jour automatique des signatures antivirus.

Cliquez sur le bouton **Se connecter au serveur** si vous n'êtes pas encore enregistré sur le serveur G DATA. Il vous suffit de saisir la clé de licence qui vous a été fournie lors de l'achat et vos données client, puis de cliquer sur **Se connecter**. Vos codes d'accès (nom d'utilisateur et mot de passe) sont alors affichés. Vous devez noter ces données et les conserver soigneusement. Une connexion Internet est évidemment nécessaire à l'enregistrement de votre licence (tout comme pour la mise à jour Internet des signatures antivirus).

Planification de la mise à jour Internet (base de données des virus)

L'onglet Planification de la mise à jour Internet (base de données des virus) permet de définir quand et à quel rythme la mise à jour automatique doit avoir lieu. Choisissez la fréquence sous **Fréquence**, puis définissez les paramètres correspondants sous **Date/heure**.

L'option **Tous les jours**, avec l'aide des indications sous **Jours de la semaine**, vous permet par exemple de définir si la mise à jour n'est exécutée que durant les jours ouvrables, tous les deux jours ou le week-end. Pour modifier les dates et les heures définies sous **Date/heure**, il vous suffit de sélectionner l'élément que vous souhaitez modifier (par exemple, le jour, l'heure, le mois ou l'année) à l'aide de la souris et d'en déplacer la fréquence sur la frise chronologique à l'aide des touches fléchées ou de l'icône en forme de flèche située à droite du champ de saisie.

Paramètres Internet

Si vous utilisez un ordinateur protégé par un pare-feu ou soumis à d'autres paramètres particuliers en rapport avec votre connexion Internet, veuillez indiquer un **Serveur proxy**. Ne modifiez ce réglage que si la mise à jour Internet ne fonctionne pas. Pour connaître votre adresse proxy, veuillez-vous adresser à votre fournisseur d'accès à Internet.

Les codes d'accès pour la connexion à Internet (nom d'utilisateur et mot de passe) sont très importants pour la mise à jour automatique. Sans ces données, la connexion automatique à Internet ne peut pas être établie. Veillez également à ce que vos paramètres Internet généraux (pour votre programme de messagerie électronique ou votre navigateur Internet, par exemple) autorisent la numérotation automatique. Sans la numérotation automatique, G DATA MailSecurity démarre la procédure de mise à jour Internet mais l'application doit ensuite attendre que vous confirmiez l'établissement de la connexion Internet en cliquant sur **OK**. Sous **Région du serveur de mise à jour**, vous pouvez sélectionner un serveur de mise à jour dans votre région de manière à optimiser la transmission de données.

Compte utilisateur
Veuillez saisir un compte utilisateur défini sur l'ordinateur MAILGATEWAY et pour lequel il existe un accès Internet sous **Compte utilisateur**.

> **Attention** : veuillez ne pas confondre les données saisies au niveau des onglets **Codes d'accès** et **Compte utilisateur**.

12.2.2.2. Signatures de virus

Les boutons **Actualiser la base de données des virus** et **Actualiser le statut** vous permettent de lancer la mise à jour des signatures antivirus indépendamment des données saisies pour la planification.

12.2.2.3. Fichiers programmes

Le bouton **Mise à jour du programme** vous permet de mettre les fichiers du programme G DATA MailSecurity à jour lorsque des modifications ou des améliorations sont apportées.

12.3. Rubriques du programme

Le fonctionnement du programme G DATA MailSecurity est en principe clair et facile à comprendre. Les différents onglets que vous pouvez sélectionner à l'aide des icônes affichées sur la gauche dans l'application G DATA MailSecurity Administrator vous permettent d'accéder à la rubrique du programme souhaité et d'y exécuter des actions, de procéder à des réglages ou d'analyser des processus.

12.3.1. État

La rubrique État de l'application Administrator contient des informations de base au sujet du statut du système et de la passerelle de messagerie. Elles apparaissent à droite de chaque entrée, sous la forme de texte, de données chiffrées ou de dates.

- Si votre application G DATA MailSecurity est configurée de manière optimale pour la protection contre les virus informatiques, une coche verte s'affiche à gauche des entrées.
- Si un composant n'est pas réglé de manière optimale (signatures trop anciennes, analyses antivirus désactivées, par exemple), une icône d'alerte vous le signale.

Double-cliquez sur les éléments correspondants (ou sélectionnez les éléments et cliquez ensuite sur le bouton **Modifier**) pour exécuter directement des actions ou accéder à la zone correspondante du programme. Une fois la configuration d'un élément doté de l'icône d'alerte optimisée, une icône de feu de signalisation vert s'affiche dans la rubrique Statut. Les options suivantes vous sont proposées :

- **Traitement du courrier entrant** : le traitement du courrier entrant permet de garantir la vérification des courriers à l'aide de la passerelle de messagerie avant leur transmission au destinataire. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Options** > **Entrant (SMTP)** et **Options** > **Entrant (POP3)**) et vous pouvez adapter le traitement du courrier entrant à vos besoins.
- **Vérification antivirus du courrier entrant** : la vérification des courriers entrants permet d'éviter que des courriers infectés n'infiltrent votre réseau. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Options** > **Analyse antivirus**) et vous pouvez adapter la vérification des courriers entrants à vos besoins.
- **Traitement du courrier sortant** : le traitement des courriers sortants permet de garantir la

vérification des courriers à l'aide de la passerelle de messagerie avant leur transmission au destinataire. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Options** > **Sortant (SMTP)**) et vous pouvez adapter le traitement du courrier entrant à vos besoins.

- **Vérification antivirus du courrier sortant** : la vérification des courriers sortants permet d'éviter que des fichiers infectés ne soient envoyés à partir de votre réseau. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Options** > **Analyse antivirus**) et vous pouvez adapter la vérification des courriers sortants à vos besoins.
- **OutbreakShield** : la technologie OutbreakShield permet de détecter et de combattre les programmes malveillants dans les envois massifs de messages électroniques avant que les signatures correspondantes ne soient disponibles. Cette technologie surveille le trafic mondial de courriers électroniques et identifie les pics d'envoi de courriers suspects. Selon une multitude de critères, les courriers dangereux sont identifiés et bloqués ce qui lui permet de combler quasiment en temps réel le laps de temps entre le début d'un envoi massif de messages électroniques infectés et son traitement au moyen de signatures adaptées.
- **Mises à jour automatiques** : les signatures antivirus peuvent être automatiquement mises à jour. Vous devez activer l'option des mises à jour automatiques. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Mise à jour**) et vous pouvez adapter la fréquence des mises à jour à vos besoins.
- **Date des signatures de virus** : plus les signatures antivirus sont récentes, plus la protection antivirus est efficace. Vous devez mettre les signatures antivirus à jour aussi souvent que possible et automatiser ce processus autant que possible. Si vous double-cliquez sur cette entrée, la fenêtre de paramétrage correspondante s'affiche (barre de menus : **Mise à jour**) et vous pouvez procéder directement à une mise à jour Internet (indépendamment de l'automatisation programmée).
- **Filtre antispam** : le filtre antispam vous offre la possibilité de bloquer les messages à contenu non désiré ou d'expéditeurs non désirés (expéditeurs de masse, par exemple).
- **Spam-OutbreakShield** : Spam-OutbreakShield permet de détecter et de lutter contre les courriers électroniques envoyés en masse. Avant de collecter les courriers, la technologie Spam-OutbreakShield interroge une base de spam et ne transmet alors à la boîte de réception du destinataire que les emails légitimes.

Si vous avez activé l'option Statistiques de la messagerie électronique lors de l'installation, vous pouvez accéder à l'analyse statistique de vos courriers électroniques entrants et sortants ou du spam en cliquant sur le bouton **Statistiques**. La configuration des statistiques est assurée dans le menu **Options** de l'application Administrator, sous l'onglet **Journalisation**.

12.3.2. Filtre

La rubrique Filtre vous permet d'utiliser aisément des filtres qui bloquent les courriers entrants ou sortants ou qui suppriment automatiquement les contenus potentiellement dangereux. Les filtres en question sont répertoriés dans la liste de la rubrique Filtre et peuvent être activés ou désactivés à l'aide des cases à cocher situées à gauche de chaque entrée.

- **Importer** : vous pouvez importer des filtres et leurs paramètres spéciaux depuis un fichier XML.
- **Exporter** : vous pouvez enregistrer des filtres et leurs paramètres spéciaux en tant que fichiers XML et les réutiliser sur un autre ordinateur. Pour exporter plusieurs filtres, utilisez la souris et maintenez la touche CTRL enfoncée.

- **Nouveau** : le bouton Nouveau permet la définition de nouvelles règles de filtrage. Lorsque vous ajoutez un nouveau filtre, une fenêtre de sélection s'affiche et vous demande de déterminer le type de filtre de base. Vous pouvez ainsi saisir toutes les données supplémentaires de filtre à créer dans une fenêtre d'assistance adaptée à ce type de filtre. Vous pouvez aisément installer des filtres contre tous les types de dangers.
- **Modifier** : le bouton Modifier permet de modifier les filtres existants.
- **Supprimer** : pour supprimer définitivement un filtre, il vous suffit de le sélectionner d'un clic et de cliquer sur le bouton Supprimer.
- **Statistiques** : vous pouvez consulter les statistiques de chaque filtre.
- **Journal** : pour le filtre antispam, il existe un journal avec une liste dans laquelle les courriers considérés comme du spam sont répertoriés. Le journal vous permet également d'identifier les critères à l'origine de l'identification en tant que spam (valeurs de l'index de spam). Si un courrier est considéré comme du spam de manière injustifiée, vous pouvez informer le serveur OutbreakShield en ligne qu'il s'agit d'une erreur de détection (faux positif). Le courrier sera ensuite de nouveau vérifié par OutbreakShield. S'il a effectivement été identifié comme un spam de manière erronée, il sera classé comme ne présentant aucun risque. Seule une somme de contrôle est transmise (et non le contenu du courrier).

  Votre réseau est également protégé contre les attaques de virus indépendamment des règles de filtrage. En effet, G DATA MailSecurity vérifie en permanence en arrière-plan les courriers électroniques entrants et sortants. Les règles de filtrage permettent cependant de protéger vos comptes de messagerie électronique des courriers indésirables, du spam et des scripts dangereux et de minimiser les foyers de virus éventuels avant leur détection par G DATA MailSecurity.

Généralement, vous avez la possibilité d'attribuer un nom spécifique à chaque filtre sous **Nom**. C'est sous ce nom que ce filtre s'affiche dans la liste de la rubrique Filtre. La rubrique **Remarque** vous permet d'ajouter des notes ou commentaires au filtre concerné. Sous **Sens**, vous pouvez généralement définir si une règle de filtrage s'applique uniquement aux **Courriers entrants**, uniquement aux **Courriers sortants** ou dans les deux sens.

La rubrique **Réaction** permet de préciser comment sont traités les courriers reconnus comme spam une fois les critères de filtrage définis. Vous pouvez alors définir le texte des fonctions **Notifier l'expéditeur du message** et **Envoyer le message aux personnes suivantes**. Pour ce faire, il vous suffit de cliquer sur le bouton situé sur la droite de la réaction souhaitée. Vous pouvez utiliser des caractères génériques pour ajouter des informations dans les champs **Objet** et **Corps du courrier**. Il s'agit des mêmes caractères génériques que ceux utilisés dans la rubrique **Entrant (POP3)** > **Filtre**.

12.3.2.1. Filtrer la confirmation de lecture

Ce filtre supprime les demandes de confirmation de lecture pour les courriers électroniques entrants ou sortants.

12.3.2.2. Désactiver les scripts HTML

Ce filtre sert à désactiver les scripts dans la partie HTML du message. Les scripts, dont toute l'utilité repose sur leur présence sur un site Internet, sont, lorsqu'ils sont intégrés à un courrier électronique HTML, plutôt dérangeants. Les scripts HTML sont parfois également utilisés pour contaminer les ordinateurs. Ces scripts ont alors la possibilité de faire effet dès l'affichage du message électronique, et pas seulement après l'ouverture de la pièce jointe infectée.

12.3.2.3. Désactiver les références externes

De nombreuses lettres d'information au format HTML incluent des liens, affichés et exécutés lors de l'ouverture du message. Il peut s'agir, par exemple, d'illustrations qui ne sont pas envoyées avec le courrier, mais qui peuvent être automatiquement téléchargées via un hyperlien. Étant donné qu'il ne s'agit pas uniquement d'illustrations inoffensives mais parfois également de routines nuisibles, il peut être utile de désactiver ces références. Le texte du message n'est pas affecté par la désactivation.

12.3.2.4. Filtre de la liste grise

Le filtre de la liste grise est un bon moyen de limiter le spam. Les courriers électroniques provenant d'expéditeurs inconnus ne sont alors pas immédiatement transférés au destinataire par le biais du serveur SMTP lors de la première tentative de distribution. Les expéditeurs de spam ne gèrent généralement pas les files d'attente et tentent rarement d'envoyer leurs courriers électroniques une deuxième fois au même serveur SMTP, le nombre de courriers de spam transférés peut donc être réduit de manière considérable.

- **Délais d'attente (minutes)** : ces paramètres vous permettent de définir la durée pendant laquelle la transmission des courriers suspects est bloquée. Une fois ce laps de temps écoulé, les courriers sont transférés en cas de nouvelle tentative d'envoi. Si le destinataire répond à l'expéditeur, ce dernier est déplacé de la liste grise vers une liste blanche. La distribution des courriers électroniques n'est alors plus bloquée, ni retardée.
- **Durées de vie (jours)** : pour que la liste blanche des expéditeurs désirables soit en permanence à jour, les adresses des expéditeurs ne restent qu'un certain temps dans la liste blanche, elles sont ensuite de nouveau transférées dans la liste grise. La minuterie est réinitialisée pour chaque expéditeur, à chaque nouvel envoi de courrier. Si vous saisissez ici une valeur de plus de 30 jours, par exemple, les lettres d'information mensuelles que vous souhaitez recevoir sont intégrées en permanence à la liste blanche.

  Le filtre de la liste grise ne peut être sélectionné que lorsque l'option **Filtre antispam** de l'application G DATA MailSecurity est activée. En outre, une base de données SQL doit être installée sur le serveur.

12.3.2.5. Filtrage des pièces jointes

Les filtres des pièces jointes vous offrent un grand nombre de possibilités de blocage des pièces jointes. La plupart des virus de courrier électronique se propagent via des pièces jointes qui, dans la plupart des cas, contiennent des fichiers exécutables plus ou moins bien cachés. Il peut s'agir de simples fichiers EXE contenant un programme malveillant, mais également de scripts VB se dissimulant parfois derrière des fichiers images, vidéo ou audio. Les utilisateurs doivent prendre toutes les précautions nécessaires avant d'ouvrir une pièce jointe et, en cas de doute, il est préférable de demander la confirmation d'un courrier électronique à l'expéditeur avant d'ouvrir le fichier joint.

Sous **Extensions de fichier**, vous pouvez indiquer les extensions de fichiers que vous souhaitez ajouter au filtre. Vous pouvez regrouper dans un filtre tous les fichiers exécutables (les fichiers EXE et COM, par exemple). Vous pouvez cependant également filtrer d'autres formats (MPEG, AVI, MP3, JPEG, JPG, GIF, etc.) au cas où leur taille surchargerait votre serveur de messagerie. Vous pouvez également filtrer les fichiers d'archives (ZIP, RAR ou CAB, par exemple). Utilisez des points-virgules pour séparer les différentes extensions de fichiers d'un groupe de filtrage (**.exe ; *.dll*, par exemple). Indiquez sous Mode si vous souhaitez autoriser (**Autoriser uniquement les pièces jointes indiquées**) ou bloquer (**Filtrer les pièces jointes indiquées**) les extensions de fichiers répertoriées sous Extensions de

fichier.

Avec la fonction **Filtrer également les pièces jointes des courriers intégrés**, le filtrage des pièces jointes sélectionnées sous Extensions de fichier s'effectue également dans les courriers constituant eux-mêmes une pièce jointe. Cette option doit en règle générale être activée. L'option **Ne renommer que les pièces jointes** ne supprime pas automatiquement les pièces jointes à filtrer mais les renomme uniquement. Cela peut s'avérer utile dans le cas de fichiers exécutables (comme les fichiers EXE et COM), mais aussi de fichiers Microsoft Office, pouvant éventuellement renfermer des scripts et des macros exécutables. En renommant les pièces jointes, vous évitez toute appréciation hâtive qui amènerait l'utilisateur à ouvrir la pièce jointe sans réfléchir. Avant de pouvoir l'utiliser, le destinataire du message doit d'abord enregistrer la pièce jointe et la renommer. Si la case Ne renommer que les pièces jointes n'est pas cochée, les pièces jointes correspondantes sont directement supprimées.

Le champ **Suffixe** vous permet de définir la chaîne de caractères à ajouter à l'extension de fichier initiale et d'empêcher ainsi l'exécution accidentelle d'un fichier via un simple clic de souris (**.exe_danger*, par exemple). Grâce au champ **Insérer le texte suivant dans le message**, vous pouvez informer le destinataire du message filtré qu'une pièce jointe a été supprimée ou renommée conformément à une règle de filtrage.

12.3.2.6. Filtrage du contenu

Grâce au filtrage du contenu, vous pouvez facilement bloquer des messages abordant un sujet ou contenant des mots particuliers. Pour ce faire, il vous suffit de saisir, sous **Expression réglementaire**, les mots-clés et les expressions auxquels G DATA MailSecurity doit réagir. Indiquez également sous **Domaine de recherche** les sections des messages dans lesquelles le programme doit rechercher ces expressions. Le bouton **Nouveau**, situé à droite du champ de saisie Expression réglementaire, vous permet de saisir facilement le texte de filtrage. Pour ce faire, vous pouvez lier à volonté un texte avec les opérateurs logiques *ET* et *OU*.

> Si vous saisissez *alcool ET drogue*, les messages contenant les termes *alcool* et *drogue* sont filtrés, mais pas les messages contenant uniquement le terme *alcool* ou le terme *drogue*. L'opérateur logique ET définit que tous les éléments reliés par ET doivent exister et l'opérateur OU qu'au moins un des éléments doit être présent.

Sous Expression réglementaire, vous pouvez également associer les critères de recherche à votre guise, sans l'aide à la saisie. Il suffit pour cela de saisir les critères de recherche et de les associer à l'aide des opérateurs logiques. L'opérateur "ou" est représenté par la barre de séparation "|" (AltGr + 6). L'opérateur "et" est représenté par le et commercial "&" (Maj + 6).

12.3.2.7. Filtrage de l'expéditeur

Grâce au filtrage de l'expéditeur, vous pouvez facilement bloquer les messages provenant de certains expéditeurs. Pour ce faire, il vous suffit de saisir, sous **Adresses/domaines**, les adresses électroniques ou les noms de domaine qui doivent faire réagir le logiciel G DATA MailSecurity. Vous pouvez saisir plusieurs entrées en les séparant par des points-virgules. Vous pouvez également filtrer automatiquement les messages ne contenant aucune indication relative à l'expéditeur.

12.3.2.8. Filtre des destinataires

Le filtre des destinataires vous permet de bloquer facilement la réception des courriers électroniques par certains destinataires. Pour ce faire, il vous suffit de saisir, sous **Adresses/domaines**, les adresses électroniques ou les noms de domaine qui doivent faire réagir le logiciel G DATA MailSecurity. Vous

pouvez saisir plusieurs entrées en les séparant par des points-virgules. Vous pouvez également filtrer automatiquement les messages avec un champ de destinataire vide (les messages qui contiennent uniquement des destinataires en Cci et/ou en Cc).

12.3.2.9. Filtrage anti-spam

Le filtre antispam vous propose de nombreux paramètres vous permettant de bloquer les courriers électroniques contenant des contenus indésirables ou provenant d'expéditeurs indésirables (expéditeurs de masse, par exemple). Le programme contrôle de nombreux critères du message qui relèvent typiquement du courrier indésirable. Ces différents critères évalués résultent en une valeur qui reflète leur probabilité d'être du courrier indésirable. Vous disposez de plusieurs onglets où tous les paramètres pertinents sont classés par thèmes.

Filtre

Si vous souhaitez nommer le filtre et saisir des précisions supplémentaires, utilisez les champs **Nom** et **Remarque**. La section **Réaction** vous permet de choisir le comportement du filtre antispam face aux messages suspectés d'être des spams. Vous pouvez influencer le comportement du filtre antispam en fonction de trois types de menaces, définis par le degré de probabilité de spam établi par G DATA MailSecurity.

Le groupe **Soupçon spam** contient les messages dans lesquels G DATA MailSecurity a détecté des éléments de spam. Les messages classés ici ne sont pas forcément du spam, il peut s'agir dans de rares cas de lettres d'information ou de mailings souhaités par le destinataire. Il est recommandé ici de signaler au destinataire que le message est suspecté d'être un spam. Le groupe **Probabilité élevée de spam** rassemble les messages associant de nombreuses marques distinctives de spam. Il s'agit très rarement de messages souhaités par le destinataire. Le groupe **Probabilité très élevée de spam** contient les messages remplissant tous les critères d'un spam. Il s'agit en général de messages non désirés et le rejet de ce type de messages est recommandé dans la plupart des cas. Ces trois types de menaces peuvent être paramétrés individuellement.

Utilisez l'option **Refuser le message** si vous souhaitez que les messages ne soient pas transmis à votre serveur de messagerie. Le destinataire ne reçoit alors pas les messages. L'option **Insérer l'avertissement de spam dans l'objet et le texte du message** vous permet d'informer le destinataire d'un message identifié comme spam qu'il s'agit d'un spam. Avec l'option **Notifier l'expéditeur du message**, vous pouvez envoyer une réponse automatique à l'expéditeur du message identifié comme spam de manière à l'informer que son e-mail a été traité comme un spam. Étant donné que le spam utilise souvent de nombreuses adresses électroniques, vous devez réfléchir avant d'activer cette fonction. L'option **Transmettre aux personnes suivantes** vous permet de transmettre automatiquement le courrier indésirable à l'administrateur du système, par exemple.

Liste blanche

La liste blanche vous permet d'exclure explicitement de la vérification antispam les adresses de certains expéditeurs ou de certains domaines. Il vous suffit, pour ce faire, de saisir, dans le champ **Adresses/domaines**, l'adresse électronique (newsletter@gdata.fr, par exemple) ou le domaine (gdata.fr, par exemple) que vous souhaitez traiter en tant qu'exception, le programme G DATA MailSecurity ne considère alors plus les courriers électroniques provenant de cet expéditeur ou de ce domaine comme du spam. Le bouton **Importer** vous permet d'ajouter à la liste blanche des listes prédéfinies d'adresses électroniques ou de noms de domaine. Les adresses et les domaines de ces listes doivent se présenter les uns en dessous des autres sur des lignes individuelles. Le format utilisé est celui d'un fichier texte, pouvant être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter une telle liste blanche sous la forme d'un fichier texte.

Liste noire

La liste noire vous permet de définir explicitement comme étant du spam les messages provenant des adresses de certains expéditeurs ou de certains domaines. Pour ce faire, il vous suffit de saisir, dans le champ **Adresses/domaines**, l'adresse électronique (newsletter@megaspam.fr.vu, par exemple) ou le domaine (megaspam.fr.vu, par exemple) que vous soupçonnez de spam. G DATA MailSecurity traite alors les courriers de l'expéditeur ou du domaine comme des courriers présentant une très forte probabilité de spam. Le bouton **Importer** vous permet d'ajouter à la liste noire des listes prédéfinies d'adresses électroniques ou de domaines. Les adresses et les domaines de ces listes doivent se présenter les uns en dessous des autres sur des lignes individuelles. Le format utilisé est celui d'un simple fichier texte, pouvant, par exemple, être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter la liste noire en tant que fichier texte.

Listes noires en temps réel

Vous pouvez trouver sur Internet des listes noires contenant les adresses IP de serveurs qui permettent l'expédition de spam. G DATA MailSecurity détermine, par le biais de requêtes DNS sur les listes noires en temps réel, si le serveur à l'origine de l'expédition y est répertorié. Si tel est le cas, la probabilité de spam augmente. Il est généralement recommandé d'utiliser ici les paramètres standards ; vous avez cependant la possibilité d'assigner aux **Listes noires 1**, **2** et **3** vos propres adresses issues d'Internet en tant que listes noires.

Mots-clés (champ Objet)

La liste des mots-clés vous permet également d'utiliser les mots de la ligne d'objet des courriers électroniques pour détecter le spam. Si au moins un des termes est présent dans la ligne de l'objet, la probabilité d'être en présence d'un spam augmente. Cette liste peut être modifiée à volonté à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Le bouton **Importer** vous permet d'ajouter des listes préétablies de mots-clés. Les entrées figurant dans ces listes doivent se présenter les unes au-dessous des autres sur des lignes individuelles. Le format utilisé est celui d'un fichier texte, pouvant être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet aussi d'exporter une telle liste de mots-clés sous la forme d'un fichier texte. La case **Rechercher uniquement les mots entiers** vous permet d'ordonner à G DATA MailSecurity de rechercher dans la ligne de l'objet d'un message uniquement des mots entiers. Ainsi, une expression telle que *argent* est soupçonnée d'être un spam, tandis que les mots contenant ce radical, comme *argenterie*, ne le sont pas.

Mots clés (corps du message)

La liste des mots-clés vous permet d'utiliser les mots du corps du message dans le cadre de la suspicion de spam. Si au moins un des termes est présent dans le texte du message, la probabilité d'être en présence d'un spam augmente. Cette liste peut être modifiée à volonté à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Le bouton **Importer** vous permet d'ajouter des listes préétablies de mots-clés. Les entrées figurant dans ces listes doivent se présenter les unes au-dessous des autres sur des lignes individuelles. Le format utilisé est celui d'un fichier texte, pouvant être créé avec l'outil Bloc-notes de Windows. Le bouton **Exporter** vous permet d'exporter une telle liste de mots-clés sous forme de fichier texte. La case **Rechercher uniquement les mots entiers** vous permet d'ordonner à G DATA MailSecurity de rechercher dans la ligne de l'objet d'un message uniquement des mots entiers. Ainsi, une expression telle que *argent* est soupçonnée d'être un spam, tandis que les mots contenant ce radical, comme *argenterie*, ne le sont pas.

Filtrage du contenu

Le filtre de contenu est un filtre autodidacte basé sur la méthode Bayes, qui calcule la probabilité de spam à partir des mots utilisés dans le corps du courrier. Ce filtre ne se contente pas de travailler avec des listes exhaustives de mots : il étoffe ses connaissances à chaque nouveau message réceptionné.

Le bouton **Rechercher dans les contenus des tableaux** permet d'afficher les listes de mots utilisées par le filtre de contenu pour classer un message dans la catégorie des spams. Le bouton **Rétablir les tableaux initiaux** permet d'effacer le contenu des tableaux appris, le filtre de contenu recommence alors la procédure d'apprentissage depuis le début.

Paramètres avancés
Cette rubrique vous permet de modifier en détail la détection des spams de G DATA MailSecurity et de l'adapter aux conditions de votre serveur de messagerie. Il est toutefois recommandé d'utiliser les paramètres standards dans la majorité des cas. Modifiez les paramètres avancés uniquement si vous maîtrisez le sujet et si vous savez exactement ce que vous faites.

Sélectionnez l'option **Valeurs de l'index de spam** pour modifier les valeurs utilisées pour classer les courriers électroniques en fonction de la probabilité de spam. Nous vous recommandons d'utiliser les valeurs standards.

12.3.2.10. Filtre IP

Le filtre IP bloque la réception des courriers expédiés par certains serveurs. Le filtre peut être utilisé en mode liste noire ou liste blanche. Sous **Nom** et **Remarque**, indiquez la raison pour laquelle vous souhaitez bloquer ou autoriser les adresses IP correspondantes. Saisissez ensuite les adresses IP sous **Adresses IP**. Cliquez sur **Ajouter**, les adresses IP saisies sont alors ajoutées à la liste des adresses IP bloquées. Sous Mode, vous pouvez indiquer si le filtre IP doit autoriser des plages d'adresse IP en mode liste blanche ou bloquer des plages d'adresses IP en mode liste noire. Vous pouvez exporter la liste des adresses IP sous forme de fichier TXT ou importer une liste d'adresses IP au format TXT.

12.3.2.11. Filtrage langues

Le filtre linguistique vous permet de définir automatiquement certaines langues comme spam. Généralement, si vous n'êtes en contact avec aucun correspondant anglophone, vous pouvez définir tout message en anglais comme courrier indésirable, ce qui vous épargnera de nombreux spams. Dans ce cas, choisissez simplement les langues dont vous n'attendez pas de messages réguliers. G DATA MailSecurity augmente alors considérablement l'estimation de probabilité de spam pour ces messages.

12.3.3. Files d'attente

Dans la rubrique Files d'attente, vous accédez à tout moment à un aperçu des courriers entrants et sortants qui transitent par la passerelle de messagerie et qui sont soumis à l'analyse antivirus et/ou du contenu. Les courriers sont généralement immédiatement transmis, légèrement retardés par le passage via la passerelle de messagerie, et sont donc immédiatement supprimés de la liste des files d'attente. Si un courrier ne peut pas être distribué ou s'il existe des retards de distribution (parce que le serveur concerné est momentanément indisponible, par exemple), une entrée correspondante est ajoutée à la liste des files d'attente. G DATA MailSecurity tente alors d'envoyer de nouveau le courrier à des intervalles qui peuvent être définis (sous **Options** > **File d'attente**).

Les distributions retardées ou ayant échoué sont ainsi toujours documentées. Le bouton **Entrant/ sortant** vous permet de basculer entre la liste des courriers entrants et la liste des courriers sortants. Le bouton **Répéter maintenant** vous permet de distribuer de nouveau un courrier sélectionné qui n'a pas pu être distribué, indépendamment de l'heure sélectionnée pour la redistribution sous **Options** > **File d'attente**. Le bouton **Supprimer** vous permet de supprimer définitivement un courrier non distribué de la file.

12.3.4. Activité

Dans la rubrique Activité, vous accédez à tout moment à un aperçu des actions effectuées par G DATA MailSecurity. Les actions sont répertoriées avec l'**Heure**, l'**ID** et l'**Action** dans la liste des activités. Les barres de défilement situées sur la droite vous permettent de faire défiler le journal. Le bouton **Rétablir** vous permet de supprimer le protocole créé. G DATA MailSecurity redémarre alors l'enregistrement des activités. La fonction **Désactiver le défilement** permet d'actualiser la liste, mais les dernières activités ne sont pas placées directement en position de tête. Vous pourrez ensuite faire défiler la liste avec plus de concentration.

> L'ID permet d'affecter distinctement les actions enregistrées à des courriers précis. Les procédures disposant du même identifiant sont toujours regroupées (12345 Chargement du courrier, 12345 Traitement du courrier, 12345 Envoi du courrier, par exemple).

12.3.5. Virus détectés

La rubrique Virus détectés vous fournit des informations détaillées en cas de détection d'un courrier infecté par G DATA MailSecurity, au sujet des mesures prises, du type de virus dont il s'agit et de l'identité de l'expéditeur et du destinataire du courrier en question. L'option **Supprimer** vous permet de supprimer la notification de virus sélectionnée de la liste des virus détectés.

13. FAQ

13.1. Installation

13.1.1. Après installation du client, certaines applications sont nettement plus lentes qu'avant

L'outil de surveillance contrôle en arrière-plan l'accès à l'ensemble des fichiers et s'assure de l'absence de virus dans les fichiers en cours d'accès. Ce processus consomme des ressources, mais reste toutefois à peine perceptible. Mais si une application ouvre très fréquemment des fichiers ou ouvre un grand nombre de fichiers, un retard plus important peut être généré sur cette application. Pour éviter ce problème, désactivez temporairement l'outil de surveillance afin de déterminer s'il est vraiment à l'origine de ce ralentissement. Si l'ordinateur concerné accède aux fichiers d'un serveur, vous devez également désactiver temporairement l'outil de surveillance sur le serveur. Si l'outil de surveillance est la cause, la création d'une exception (fichiers qui ne doivent pas être vérifiés) peut résoudre le problème. Pour ce faire, vous devez identifier les fichiers auxquels vous accédez fréquemment. Vous pouvez identifier ces données à l'aide d'un programme tel que MonActivity, par exemple. Adressez-vous pour ce faire à notre **ServiceCenter**.

> Vous pouvez également augmenter le niveau de performances en utilisant un seul moteur, à la place des deux, pour l'analyse antivirus. Cela peut être une solution sur les systèmes plus anciens. Le réglage peut être effectué dans la rubrique **Outil de surveillance**.

13.1.2. J'ai installé le logiciel G DATA sans l'enregistrer. Comment puis-je enregistrer le logiciel ?

Pour enregistrer ultérieurement le logiciel, sélectionnez l'option **Mise à jour Internet** sous **Démarrer** > **Tous les programmes** > **G DATA** > **G DATA ManagementServer**. L'option **Enregistrement en ligne** est alors à votre disposition. Cliquez sur le bouton pour ouvrir le formulaire d'enregistrement. Saisissez le numéro d'enregistrement fourni avec la solution. Le numéro se trouve sur la confirmation de commande. En cas de doutes, contactez votre revendeur ou le distributeur responsable.

La saisie du numéro d'enregistrement permet d'activer la solution. Les données d'accès créées sont affichées une fois l'enregistrement correctement effectué. **Vous devez impérativement noter ces codes d'accès !** Il n'est plus possible de saisir de nouveau la clé de licence une fois l'enregistrement correctement effectué. Si vous rencontrez des problèmes lors de la saisie du numéro d'enregistrement, vérifiez que le numéro d'enregistrement a été correctement saisi. Selon la typographie utilisée, un grand l (Inès) peut être confondu avec le chiffre 1 ou la lettre L (Louis). Cela est également le cas pour : B et 8, G et 6, Z et 2.

> Si vous avez acheté une application G DATA Client Security Business ou G DATA Endpoint Protection Business ou un module complémentaire G DATA PatchManager sans l'activer lors de l'installation, les onglets Pare-feu, PatchManager et PolicyManager ne s'affichent qu'une fois l'activation correctement effectuée. Seules les fonctions de l'application G DATA Antivirus Business sont disponibles en attendant.

13.1.3. MailSecurity for Exchange

13.1.3.1. MailSecurity, Exchange Server 2007

Lors de la mise à niveau de MailSecurity pour Exchange sur Microsoft Exchange Server 2007, Microsoft. NET Framework 3.5 ou plus récent doit être présent. Si Microsoft .NET Framework 3.5 ou plus récent n'est pas présent, GDVSService ne se lancera après la mise à jour. Installer Microsoft .NET

Framework 3.5 ou plus récent avant ou après la mise à niveau de MailSecurity pour Exchange garantira la pleine fonctionnalité.

13.1.3.2. Mise à jour de la version 12

À cause de changements dans la procédure d'installation, les installations MailSecurity pour Exchange, déployées initialement à partir de la version 12 ne peuvent être mises à jour vers la version 14, même si elles ont été déjà mises à jour vers la version 13.0 ou 13.1. Dans ce cas, la version précédente de MailSecurity pour Exchange doit être désinstallée avant d'installer la version 14. De plus, il faut s'assurer que MailSecurity pour Exchange est installé sur tous les serveurs Exchange ayant le rôle de Mailbox ou de Hub Transport.

13.1.3.3. MailSecurity, Exchange Server 2000 et AVM Ken!

Si vous utilisez le serveur AVM Ken! et souhaitez installer G DATA MailSecurity sur le même ordinateur, adressez-vous à notre **équipe d'assistance** pour obtenir des informations détaillées.

Si vous utilisez le serveur Exchange Server 2000 et souhaitez installer G DATA MailSecurity sur le même ordinateur ou si vous souhaitez modifier les ports pour les courriers électroniques entrants et sortants au niveau du serveur Exchange Server, adressez-vous à notre **équipe d'assistance** pour obtenir des informations détaillées.

13.1.3.4. Installation sur un réseau avec de multiples contrôleurs de domaines

Lors de l'installation de MailSecurity pour Exchange dans un réseau avec de multiples contrôleurs de domaines Active Directory, l'assistant d'installation requiert la présence de l'utilitaire Repadmin.exe. Repadmin.exe est disponible dans le rôle domaine Active Directory, Active Directory Lightweight et l'outil de services de domaine Active Directory (Outil d'administration du serveur à distance). Avant le lancement de l'assistant d'installation de MailSecurity pour Exchange, veuillez-vous assurer qu'un ou plusieurs de ces composants sont présents.

13.2. Messages d'erreur

13.2.1. Client : « Les fichiers du programme ont été modifiés ou sont endommagés. »

Pour garantir une protection antivirus optimale, l'intégrité des fichiers du programme est régulièrement vérifiée. En cas d'erreur, le message **Les fichiers du programme ont été modifiés ou sont endommagés** s'affiche. Supprimez le message et chargez la mise à jour des fichiers du programme (G DATA Security Client) à partir de notre serveur. Procédez ensuite à l'actualisation des fichiers du programme sur les clients concernés. Contactez notre **ligne d'assistance téléphonique** si le message d'erreur s'affiche de nouveau.

13.2.2. Client : « La base de données des virus est endommagée. »

Pour garantir une protection antivirus optimale, l'intégrité de la base de données des virus est régulièrement vérifiée. En cas d'erreur, le message **La base de données des virus est endommagée** s'affiche. Effacez le message et chargez la mise à jour de la base de données des virus à partir de notre serveur. Procédez ensuite à l'actualisation de la base de données des virus sur les clients concernés. Contactez notre **ligne d'assistance téléphonique** si le message d'erreur s'affiche de nouveau.

13.2.3. « Vous devez au moins disposer de Microsoft Exchange Server 2007 SP1 pour installer l'application G DATA MailSecurity. »

Si vous voyez s'afficher le message d'erreur « Vous devez au moins disposer de Microsoft Exchange Server 2007 SP1 pour installer l'application G DATA MailSecurity. », la configuration système requise pour l'installation du plugiciel G DATA MailSecurity Exchange n'est pas respectée. Microsoft Exchange 2007 avec le Servicepack 1 est au minimum nécessaire pour l'installation. Ce programme doit être installé avant l'application G DATA MailSecurity. Voir également à ce sujet **Installation** et **Configuration système requise**.

13.3. Clients Linux

13.3.1. Installation

L'installation de G DATA Security Client pour Linux et G DATA Security Client pour Mac utilises un dépôt basé sur le ManagementServer. Lors du déploiement d'un client Linux ou Mac, les binaires concernés seront copiés du dépôt ManagementServer vers le client. S'ils ne sont pas disponibles dans le dépôt, ils seront téléchargés depuis le serveur de mises à jour G DATA, ajoutés au dépôt sur le ManagementServer et déployés ultérieurement sur le client.

13.3.2. Processus d'arrière-plan

Vérifiez que les deux processus de G DATA Security Client pour Linux fonctionnent en saisissant ce qui suit dans le terminal :

linux:~# *ps ax|grep av*

Les réponses doivent contenir les processus suivants :

/usr/local/sbin/gdavserver
/usr/local/sbin/gdavclientd

Vous pouvez démarrer les processus à l'aide de :

linux:~# */etc/init.d/gdavserver start*
linux:~# */etc/init.d/gdavclient start*

Vous pouvez arrêter les processus à l'aide de :

linux:~# */etc/init.d/gdavserver stop*
linux:~# */etc/init.d/gdavclient stop*

Pour ce faire, vous devez avoir les droits administrateur (root).

13.3.3. Fichiers Log

Les installations à distance de G DATA Security Client pour Linux sont enregistrées dans /var/log/gdata_install.log. Les informations log du processus gdavclientd et les erreurs dans /var/log/gdata/avclient.log. Les informations log du processus gdavserver et les erreurs dans /var/log/gdata/gdavserver.log, qui aident au diagnostic des pannes de connexion vers G DATA ManagementServer.

> Si vous souhaitez voir plus d'informations, éditez le fichier de configuration /etc/gdata/gdav.ini et /etc/gdata/avclient.cfr et réglez le *LogLevel*sur la valeur 7 (il faut l'ajouter si elle n'existe pas). Attention : si une valeur élevée est définie pour *LogLevel*, de nombreux messages

sont générés et la taille des fichiers journaux prend rapidement des proportions considérables. En mode de fonctionnement normal, réglez toujours LogLevel sur une faible valeur !

13.3.4. Test du serveur d'analyse

Utilisez l'outil de commande **gdavclientc** pour tester la fonctionnalité du scanner gdavserver. Les informations de versions peuvent être extraites en utilisant les commandes *baseinfo* et *coreinfo*. Exécutez un test du scanner en utilisant la commande *scan:<path>*. Voir le chapitre **gdavclientc** pour plus d'informations.

13.3.5. Connexion à G DATA ManagementServer

La communication avec G DATA ManagementServer est configurée dans : /etc/gdata/avclient.cfg. Vérifiez que l'adresse IP du ManagementServer a été entrée correctement. Si non, supprimez l'entrée incorrecte et corrigez-la directement ou relancez le client Linux par G DATA Administrator.

13.4. Autre

13.4.1. Comment puis-je vérifier que les clients sont connectés à l'application G DATA ManagementServer ?

La colonne **Dernier accès** de la rubrique des tâches **Clients** affiche l'heure à laquelle le client s'est connecté pour la dernière fois à l'application G DATA ManagementServer. Les clients se connectent normalement toutes les cinq minutes à l'application G DATA ManagementServer (si aucune tâche d'analyse n'est exécutée). L'échec de la connexion peut être lié aux causes suivantes :

- Le client est désactivé ou n'est pas connecté au réseau.
- Aucune connexion TCP/IP ne peut être établie entre le client et l'application G DATA ManagementServer. Vérifiez les paramètres du réseau ou les ports partagés.
- Le client ne peut identifier l'adresse IP du serveur (la résolution des noms DNS ne fonctionne pas). Vous pouvez vérifier la connexion à l'aide de la commande telnet. Le port TCP 7161 du serveur doit être accessible. Le port TCP 7167 ou 7169 du client doit être accessible. Vérifiez la connexion à l'aide de la commande *telnet <NOM DU SERVEUR> <NUMÉRO DE PORT>*.

  Nous attirons votre attention sur le fait que la commande telnet n'est pas disponible par défaut sous Windows Vista, Windows 7, ainsi que Server 2008 (R2). Vous devez activer la fonction Windows correspondante ou l'ajouter en tant que nouvelle fonctionnalité du serveur. Quand vous testez la connexion du client vers le serveur (*telnet <NOM DU SERVEUR> <7161>*), un ensemble de caractères spécifiques qui s'affiche dans la fenêtre indique une connexion opérationnelle. Si la connexion du serveur au client est intacte, une fenêtre de saisie vide s'affiche.

13.4.2. Ma boîte de réception a été placée en quarantaine

Cela peut se produire lorsque la boîte aux lettres contient un courrier infecté. Retour du fichier : fermez le programme de messagerie sur le client concerné et supprimez le fichier d'archivage récemment créé (le cas échéant). Ouvrez ensuite le rapport correspondant dans l'application G DATA Administrator et cliquez sur **Quarantaine : restaurer**. Veuillez contacter notre **assistance** en cas d'échec de la restauration.

13.4.3. Connexion avec ManagementServer via son adresse IP à la place de son nom

Le nom du serveur sera demandé pendant l'installation, mais il peut être remplacé par l'adresse IP si vous voulez établir une connexion vers le ManagementServer via l'adresse IP à la place de son nom. Vous pouvez également remplacer le nom du serveur par l'adresse IP ultérieurement, lorsque l'application G DATA ManagementServer est déjà installée. Pour le faire, modifiez le fichier Config.xml (localisé dans le dossier d'installation du G DATA ManagementServer) et changez la valeur pour *MainMms* vers l'adresse IP. Plus d'informations à propos de Config.xml sont situées dans le Reference Guide.

Pour que la connexion du serveur aux clients puisse également être établie à l'aide de l'adresse IP, les clients doivent être activés avec leur adresse IP dans l'application G DATA Administrator. La procédure peut être effectuée manuellement ou via la **synchronisation Active Directory**. Si vous installez les clients directement à partir du support d'installation, le programme d'installation vous demande le nom du serveur et le nom de l'ordinateur. Saisissez l'adresse IP.

13.4.4. Emplacements d'enregistrement et chemins d'accès par défaut

Signatures antivirus G DATA Security Client

- Windows XP/Server 2003/Server 2003 R2 : C:\Program Files\Common Files\G DATA\AVKScanP \BD ou G DATA
- Windows Vista/Server 2008 et versions plus récentes : C:\Programmes (x86)\Common Files \G DATA\AVKScanP\BD ou G DATA

Signatures antivirus G DATA ManagementServer

- Windows Server 2003/Server 2003 R2 : C:\Documents and settings\All Users\Application Data \G DATA\AntiVirus ManagementServer\Updates
- Windows Vista/Server 2008 et versions plus récentes : C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

Quarantaine G DATA Security Client

- Windows XP/Server 2003/Server 2003 R2 : C:\Documents and settings\All Users\Application Data \G DATA\AntiVirusKit Client\Quarantine
- Windows Vista/Server 2008 et versions plus récentes : C:\ProgramData\G DATA\AntiVirusKit Client\Quarantine

Quarantaine G DATA ManagementServer

- Windows Server 2003/Server 2003 R2 : C:\Documents and settings\All Users\Application Data \G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista/Server 2008 et versions plus récentes : C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

Bases de données G DATA ManagementServer

Windows Vista/Server 2003 et versions plus récentes :

- C:\Programmes (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_*.mdf
- C:\Programmes (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log_*.ldf

13.4.5. Comment puis-je activer un certificat de serveur SSL dans les services IIS version 7 et versions plus récentes ?

Pour garantir la sécurité des communications entre les clients et l'application WebAdministrator/ MobileAdministrator, nous vous recommandons d'ajouter un certificat de serveur SSL aux services Internet Information Services (IIS).

Pour activer un certificat de serveur SSL dans les services IIS version 7 et versions plus récentes (Windows Vista / Windows Server 2008 ou plus récent), ouvrez le **Gestionnaire des services Internet (IIS)**. Si vous utilisez Windows Server 2008, le gestionnaire IIS est disponible sous **Démarrer** > **Tous les programmes** > **Outils d'administration**. Vous pouvez également cliquer sur **Démarrer** > **Exécuter** et saisir la commande *inetmgr*.

Sélectionnez votre serveur sous **Connexions**. Sélectionnez ensuite la catégorie **IIS** et double-cliquez sur **Certificats de serveur**. Cliquez maintenant sur **Créer un certificat auto signé**. Une fois le nom du certificat saisi, le certificat est créé et affiché dans la vue d'ensemble des certificats du serveur. Nous attirons votre attention sur le fait que le certificat expire par défaut au bout d'un an (au jour près).

Pour utiliser le certificat dans le cadre de la communication, sélectionnez la page correspondante dans la rubrique **Connexions**. Dans la rubrique **Actions**, sur le côté droit, vous pouvez maintenant sélectionner les connexions. Cliquez sur **Ajouter** pour établir une nouvelle connexion. Pour le paramètre **Type**, sélectionnez https dans le menu déroulant et, sous **Certificat SSL**, sélectionnez le certificat préalablement défini. Cliquez sur **OK** pour confirmer la connexion.

L'accès aux applications WebAdministrator et MobileAdministrator via une connexion sécurisée est alors possible. Il vous suffit de remplacer le préfixe *http://*par *https://*dans votre navigateur (par exemple, *https://nom du serveur/gdadmin*). Étant donné que vous avez créé le certificat vous-même, il est possible que le navigateur affiche un avertissement avant de vous autoriser à ouvrir l'application WebAdministrator ou MobileAdministrator. La communication avec le serveur est cependant totalement chiffrée.

13.4.6. Comment puis-je activer un certificat de serveur SSL dans les services IIS version 5 ou 6 ?

Pour garantir la sécurité des communications entre les clients et l'application WebAdministrator/ MobileAdministrator, nous vous recommandons d'ajouter un certificat de serveur SSL aux services Internet Information Services (IIS).

Pour activer un certificat de serveur SSL dans les services IIS version 5 (Windows XP) ou 6 (Windows Server 2003), utilisez l'outil Microsoft SelfSSL, disponible sous IIS 6.0 Resource Kit Tools (un téléchargement gratuit est mis à disposition sur le site Web de Microsoft). Si vous exécutez le type de configuration **Custom**, vous pouvez sélectionner les outils que vous souhaitez installer. Sélectionnez **SelfSSL 1.0**. Après installation, ouvrez la ligne de commande SelfSSL via **Démarrer** > **Programmes** > **Ressources IIS** > **SelfSSL**.

Vous pouvez maintenant créer un certificat auto signé pour votre site Web en procédant à une saisie unique. Saisissez *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T* et appuyez sur **Entrée**. Confirmez la création du certificat en appuyant sur la touche **Y**. Un certificat est alors créé pour la page ISS standard sur votre serveur local et l'hôte local est ajouté à la liste des certificats dignes de confiance.

La clé compte 2 048 caractères, elle est valable pendant 365 jours précisément. Si votre page n'est pas la page ISS standard de votre serveur local, vous pouvez localiser la page correspondante sur votre

serveur, via **Démarrer** > **Outils d'administration** > **Gestionnaire des services Internet (IIS)**, et modifier le paramètre */S:1*en conséquence.

L'accès aux applications WebAdministrator et MobileAdministrator via une connexion sécurisée est alors possible. Il vous suffit de remplacer le préfixe *http://*par *https://*dans votre navigateur (par exemple, *https://nom du serveur/gdadmin*). Étant donné que vous avez créé le certificat vous-même, il est possible que le navigateur affiche un avertissement avant de vous autoriser à ouvrir l'application WebAdministrator ou MobileAdministrator. La communication avec le serveur est cependant totalement chiffrée.

14. Licences

Copyright © 2017 G DATA Software AG
Moteur A : le moteur d'analyse antivirus et les moteurs d'analyse de logiciels espions sont basés sur les technologies BitDefender technologies © 1997 -2017 BitDefender SRL.
Moteur B (CloseGap) : © 2017 G DATA Software AG
OutbreakShield : © 2017 CYREN Ltd.
Gestion des correctifs : © 2017 Lumension Security, Inc.
DevCraft Complete : © 2017 Telerik, tous droits réservés.
[G DATA - 31/08/2017, 13:53]

SharpSerializer

SharpSerializer is distributed under the New BSD License (BSD). Copyright © 2011, Pawel Idzikowski. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Polenter - Software Solutions nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Json.NET

Json.NET is distributed under The MIT License (MIT). Copyright © 2007 James Newton-King.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip

DotNetZip is distributed under the Microsoft Public License (Ms-PL).

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including

but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer,

and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index