



Guide Produit

McAfee Security for Microsoft SharePoint 3.0.0

COPYRIGHT

Copyright © 2013 McAfee, Inc. Copie sans autorisation interdite.

DROITS DE MARQUES

McAfee, le logo McAfee, McAfee Active Protection, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure sont des marques commerciales ou des marques commerciales déposées de McAfee, Inc. ou de ses filiales aux Etats-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.

Les noms et les descriptions des produits et fonctionnalités sont susceptibles d'être modifiés sans préavis. Pour en savoir plus sur les fonctionnalités et les produits les plus récents, accédez au site mcafee.com.

INFORMATIONS DE LICENCE

Accord de licence

À L'ATTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT L'ACCORD LÉGAL APPROPRIÉ CORRESPONDANT À LA LICENCE QUE VOUS AVEZ ACHETÉE, QUI DÉFINIT LES CONDITIONS GÉNÉRALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS NE CONNAISSEZ PAS LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, CONSULTEZ LES DOCUMENTS DE VENTE, D'ATTRIBUTION DE LICENCE OU LE BON DE COMMANDE QUI ACCOMPAGNENT LE LOGICIEL OU QUE VOUS AVEZ REÇUS SÉPARÉMENT LORS DE L'ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER SUR LE CD-ROM DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB À PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PACKAGE LOGICIEL). SI VOUS N'ACCEPTÉZ PAS TOUTES LES DISPOSITIONS DE CET ACCORD, NE PROCÉDEZ PAS À L'INSTALLATION DU LOGICIEL. LE CAS ÉCHÉANT, VOUS POUVEZ RETOURNER LE PRODUIT À MCAFEE OU À VOTRE REVENDEUR AFIN D'EN OBTENIR LE REMBOURSEMENT INTÉGRAL.

Sommaire

1	Introduction	7
	Fonctionnalités du produit	7
	Mode de protection du serveur SharePoint	8
2	Installation	11
	Pré-installation	11
	Configuration du système	11
	Rôles d'utilisateur	12
	Configuration système requise	13
	Types d'installation	14
	Installation standard	14
	Mise à niveau à partir d'une version précédente	16
	Tâches postérieures à l'installation	16
	Test de votre installation	16
	Test de l'analyseur à l'accès	17
	Test de l'analyseur à la demande	17
	Composants et services installés	18
3	Tableau de bord	19
	Informations statistiques des éléments détectés	19
	Détections	20
	Analyse	23
	Graphique	24
	Versions et mises à jour du produit	25
	Informations de mise à jour	25
	Planification d'une mise à jour logicielle	26
	Informations produit	26
	Licences	27
	Affichage des éléments analysés récemment	27
	Analyse à la demande	28
	Affichage de tâches d'analyse à la demande	29
	Création d'une tâche d'analyse à la demande	31
	Rapports graphiques	32
	Affichage de rapports graphiques à l'aide de filtres de recherche simples	33
	Affichage de rapports graphiques à l'aide de filtres de recherche avancés	34
4	Éléments détectés	39
	Filtres de recherche principaux	39
	Options de recherche supplémentaires	40
	Recherche parmi les éléments détectés	41
	Actions pouvant être entreprises concernant les éléments mis en quarantaine	42
5	Gestionnaire de stratégies	45
	Options de menu du gestionnaire de stratégies	45
	Catégories de stratégies de gestion des menaces	46

Types d'affichage du gestionnaire de stratégies	46
Stratégie principale et sous-stratégie	47
Création de sous-stratégies	48
Analyseurs et filtres de base	49
Affichage de la liste des analyseurs et filtres associés à une stratégie	50
Ajouter un analyseur ou un filtre	51
Créer des règles de stratégie	52
Actions pouvant être entreprises concernant les détections	53
Ressource partagée	54
Configuration des paramètres de l'analyseur	54
Configuration des paramètres d'alerte	55
Création d'une nouvelle alerte	55
Configuration des règles de conformité et DLP	58
Configuration des règles de filtrage de fichiers	61
Configuration de plages horaires	62
Gestion des paramètres d'analyseur de base d'une stratégie	63
Configuration des paramètres de l'analyseur antivirus	64
Configuration des paramètres de filtrage de fichiers	67
Configuration des paramètres d'analyseur de conformité et DLP	68
Gestion des paramètres de filtre associés à une stratégie	70
Configuration des paramètres de contenu corrompu	70
Configuration des paramètres de contenu protégé	71
Configuration des paramètres de contenu chiffré	71
Configuration des paramètres de contenu signé	72
Configuration des paramètres des fichiers protégés par mot de passe	73
Configuration des paramètres de contrôle de l'analyseur	73
6 Paramètres et diagnostics	75
Configurer la base de données de quarantaine locale pour les éléments détectés	76
Paramètres des préférences de l'interface utilisateur	78
Configuration des paramètres du tableau de bord	78
Configuration des paramètres des graphiques et diagrammes	79
Paramètres de diagnostics	80
Configuration des paramètres du journal de débogage	80
Configuration des paramètres de génération de rapports d'erreur McAfee	82
Configuration des paramètres du journal d'événements	82
Configuration des paramètres du journal du produit	83
Affichage des journaux du produit	85
Importation et exportation de paramètres de configuration	86
Importation d'une configuration du produit à partir d'un autre serveur	87
Exportation de votre configuration du produit	88
Importation d'une liste Sitelist	88
Configuration des paramètres de fichiers DAT	89
Configuration des paramètres utilisateur	89
7 Maintenance du programme	93
Réparation de l'installation	93
Purge et optimisation	94
Restauration de la configuration par défaut	95
Désinstallation du logiciel	95
8 Intégration avec ePolicy Orchestrator	97
Configuration système requise	97
Archivage du package logiciel	98
Installation des extensions logicielles	98
Migration de stratégies à partir d'une ancienne version	98

Déploiement du logiciel sur les clients	99
Gestion des stratégies	100
Créez ou modifiez des stratégies	101
Affectation de stratégies	101
Création et planification de tâches	102
Planification de mises à jour automatiques	102
Planification d'une analyse à la demande	103
Planification d'une tâche d'optimisation	103
Planification d'une tâche de purge des anciens fichiers DAT	104
Planification d'une tâche de purge	105
Requêtes et rapports	106
Requêtes prédéfinies	106
Exécution d'une requête par défaut	107
Filtrage des événements	108
Suppression du logiciel	109
Suppression du logiciel des systèmes clients	109
Suppression des extensions logicielles	110
A Création d'un compte d'utilisateur de domaine personnalisé avec des autorisations SQL minimales	113
B Editeur de liste de sites Sitelist	117
Configuration des paramètres de proxy Sitelist	118
Configuration des paramètres de référentiel Sitelist	120
C Utilisation de la fonctionnalité de contrôle d'accès	123
Index	125

1

Introduction

McAfee® Security for Microsoft SharePoint protège les données stockées sur votre serveur Microsoft SharePoint contre diverses menaces qui pourraient compromettre les ordinateurs, le réseau ou les employés.

Il analyse tous les fichiers dont le chargement ou le téléchargement s'effectue sur le serveur SharePoint. Il utilise l'analyse heuristique avancée contre les virus, le contenu indésirable, les programmes potentiellement indésirables et les types de fichiers interdits. Vous pouvez configurer les actions à prendre concernant les éléments détectés ou suspects.

Sommaire

- *Fonctionnalités du produit*
- *Mode de protection du serveur SharePoint*

Fonctionnalités du produit

Cette section décrit les principales fonctionnalités de McAfee Security for Microsoft SharePoint :

- **Protection contre les virus** — Analyse tout le contenu à la recherche de virus et protège votre serveur SharePoint en interceptant, en nettoyant et en supprimant les virus détectés. Elles utilisent des méthodes heuristiques avancées et identifient les virus inconnus ou les éléments de type viral suspectés afin de les bloquer.
- **Capacité de détection des programmes de compression et des programmes potentiellement indésirables** — Détecte les programmes de compression qui compressent et cryptent le code d'origine d'un fichier exécutable. Il détecte également les programmes potentiellement indésirables (PUP), logiciels écrits par des sociétés légales pour modifier l'état de sécurité ou de confidentialité d'un ordinateur.
- **Intégration avec McAfee® ePolicy Orchestrator® (McAfee ePO™) 4.5, 4.6 et 5.0** : s'intègre avec le serveur ePolicy Orchestrator pour fournir une méthode centralisée d'administration et de mise à jour du logiciel sur tous les serveurs SharePoint. Cela réduit le temps nécessaire pour administrer et mettre à jour les différents systèmes.
- **McAfee Global Threat Intelligence Technology (GTI)** : protège votre serveur SharePoint en offrant une sécurité en temps réel contre les menaces en constante évolution avant même qu'une signature ou mise à jour DAT soit disponible.

Dès qu'un fichier suspect est détecté sur un nœud géré protégé par un produit anti logiciels malveillants McAfee doté de la technologie GTI, elle se connecte aux serveurs McAfee en temps réel et consulte la base de données. Si le fichier suspect s'avère malveillant, le nœud géré est averti et protégé. L'interrogation et la réponse se produisent en quelques millisecondes.

Pour plus d'informations, consultez l'article [KB68631](#) de la base de connaissances McAfee.

- **Prise en charge des analyses à la demande incrémentielle** : les analyses à la demande incrémentielles gagnent du temps en n'analysant que les documents nouvellement ajoutés sur le serveur SharePoint, sans le réanalyser en totalité.

- **Prise en charge des analyses avec reprise** : analyse les documents et les dossiers depuis le dernier dossier analysé. McAfee Security for Microsoft SharePoint enregistre l'état de l'analyse. Dès que la même tâche est lancée plus tard, l'analyse reprend à partir du dernier dossier analysé.
- **Conformité et DLP** : analyse les données textuelles contenues dans les documents. Fonctionnalité garantissant que le contenu de est conforme aux stratégies de confidentialité et de conformité. Nouveautés présentées par les dictionnaires de conformité prédéfinis :
 - Ajout de 60 nouveaux dictionnaires de conformité et DLP
 - Prise en charge de dictionnaires de conformité propres au secteur : HIPAA, PCI, SourceCode (Java, C++, etc.)
 - Améliorations apportées aux détections basées sur les expressions existantes
 - Réduction des faux positifs du fait des améliorations apportées à la détection de contenu non conforme, basée sur le score du seuil et en combinaison avec le nombre maximal de termes (occurrences).

Personnalisez des stratégies pour la sécurité du contenu et de prévention des fuites de données (Data Loss Prevention, DLP).

- **Compatibilité avec l'environnement virtualisé** : cette version est prise en charge dans les environnements virtuels tels que ceux de VMware Workstation 7.0 ou version ultérieure et VMware ESX 5.x.
- **Compatibilité avec la mise à niveau** : mise à niveau à partir de McAfee Security for Microsoft SharePoint 2.5 Correctif 1 vers McAfee Security for Microsoft SharePoint 3.0 (autonome et via ePolicy Orchestrator).
- **Interface utilisateur web** : fournit une interface utilisateur web conviviale.
- **Gestion de la quarantaine** : spécifie que la base de données locale mette en quarantaine les documents infectés. Vous pouvez parcourir la base de données à la recherche de données relatives aux documents infectés.
- **Rapports** : affiche les rapports sur diverses analyses à partir du tableau de bord principal sous forme graphique.

Mode de protection du serveur SharePoint

McAfee Security for Microsoft SharePoint s'intègre avec votre serveur SharePoint et analyse tous les documents installés sur le serveur SharePoint.

Quand l'utilisateur charge les documents, SharePoint transfère ceux-ci à McAfee Security for Microsoft SharePoint.

- Le moteur d'analyse antivirus compare les documents à toutes les signatures de virus connues enregistrées dans les fichiers DAT.
- Le moteur de conformité et DLP analyse tous les documents à la recherche de contenu interdit, tel que spécifié dans les stratégies de gestion de contenu.

L'analyse a lieu chaque fois que vous créez, sauvegardez ou modifiez des données sur le serveur SharePoint. Vous pouvez également planifier des analyses pour exécution immédiate, à une heure précise ou à intervalles réguliers.

Détection en temps réel

Le logiciel vérifie les documents et les fichiers en temps réel par rapport au référentiel des fichiers DAT à jour, aux programmes malveillants et au contenu malveillant. En cas de fichiers malveillants, il envoie une notification et protège le nœud managé. Il tire parti de la technologie McAfee GTI pour empêcher les dommages et le vol de données avant même qu'une mise à jour des signatures ne soit disponible.

Détection planifiée

Vous pouvez planifier des analyses qui commencent manuellement ou à intervalles réguliers. Le logiciel vérifie tous les fichiers chargés par rapport à la dernière série de signatures de virus et de stratégies de gestion de contenu.

Analyse des documents et des dossiers sur le serveur SharePoint

- Les moteurs d'analyse antivirus et de contenu analysent les documents et présentent le résultat obtenu à McAfee Security for Microsoft SharePoint avant l'écriture du contenu le serveur Microsoft SharePoint.
- Le moteur d'analyse antivirus compare les documents à toutes les signatures connues enregistrées dans les fichiers DAT actuellement installés.
- Le moteur d'analyse de contenu analyse les documents à la recherche de contenu interdit, tel que spécifié dans les stratégies de gestion de contenu exécutées dans le logiciel. Si aucun virus ni contenu interdit/indésirable n'est présent dans les documents, il retransfert l'information au serveur SharePoint. En cas de détection, le logiciel agit comme défini dans ses paramètres de configuration.

Que doit-on analyser et quand ?

- La menace émanant des virus peut provenir de nombreuses sources telles que des macros infectées, des fichiers de programme partagés, des fichiers partagés sur un réseau, des disquettes, des fichiers téléchargés depuis Internet, etc. Les différents produits logiciels antivirus McAfee Security for Microsoft SharePoint visent des zones de vulnérabilité précises.
- McAfee Security for Microsoft SharePoint propose une série d'options que vous pouvez configurer selon les exigences de votre système. Ces exigences varient selon le moment et la façon dont les composants de votre système fonctionnent et la façon dont ils interagissent entre eux et avec le monde extérieur.
- Vous pouvez configurer ou activer les diverses actions qui vous permettent de déterminer comment votre serveur Microsoft SharePoint doit gérer différents éléments et les mesures qu'il doit prendre sur les éléments détectés ou suspects.

2

Installation

Cette section contient d'importantes informations à prendre en compte avant, pendant et après l'installation.

Sommaire


- *Pré-installation*
- *Types d'installation*
- *Tâches postérieures à l'installation*


Pré-installation

Les informations qui suivent vous permettent de préparer l'installation du produit.

Configuration du système

Assurez-vous que votre serveur répond à la configuration système requise suivante.

Composant	Configuration requise
Processeur	<ul style="list-style-type: none">• Processeur Intel x64 prenant en charge la technologie Intel Extended Memory 64 (Intel EM64T)• Processeur AMD x64 avec la technologie AMD 64 bits
Mémoire	<p> La configuration de mémoire requise pour installer ce produit est identique à celle de Microsoft SharePoint Server. Pour plus d'informations, consultez le site web de Microsoft SharePoint.</p> <ul style="list-style-type: none">• Microsoft SharePoint Server 2007 — 4 Go de RAM• Microsoft SharePoint Server 2010 — 8 Go de RAM• Microsoft SharePoint Server 2013 — 8 Go de RAM
Espace disponible sur le disque dur	740 Mo minimum d'espace disponible sur le disque dur où Microsoft SharePoint est installé.
Système d'exploitation	<ul style="list-style-type: none">• Microsoft Windows 2008 Standard/Enterprise Server SP2 (64 bits)• Microsoft Windows 2008 Standard/Enterprise Server SP1 R2 (64 bits)• Microsoft Windows 2012 Standard/Enterprise Server R2 (64 bits)

Composant	Configuration requise
Microsoft SharePoint Server	<ul style="list-style-type: none"> • Microsoft Office SharePoint Server 2007 /Windows SharePoint Services 3.0 (64 bits) • Microsoft SharePoint Server 2010 /SharePoint Foundation Server 2010 (64 bits) • Microsoft SharePoint Server 2013 /SharePoint Foundation Server 2013 (64 bits)
Navigateur	<ul style="list-style-type: none"> • Microsoft Internet Explorer versions 8.0, 9.0 et 10.0 • Mozilla Firefox versions 20.x et 21.x <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee Security for Microsoft SharePoint est certifié pour Internet Explorer et FireFox. Vous pouvez utiliser d'autres navigateurs, cependant à vos risques et périls car ils n'auront pas été testés. </div>
Résolution d'écran	Résolution 1024x768 ou supérieure (recommandée)
Logiciel de gestion McAfee	<ul style="list-style-type: none"> • McAfee ePolicy Orchestrator 4.5 • McAfee ePolicy Orchestrator 4.6 • McAfee ePolicy Orchestrator 5.0
McAfee® Agent (nécessaire pour le déploiement de McAfee ePO)	McAfee Agent 4.6 et version ultérieure
Réseau	Carte Ethernet 10/100/1000 Mbits/s

Rôles d'utilisateur

Il s'agit des rôles d'utilisateur associés à McAfee Security for Microsoft SharePoint.

Rôle	Description
Administrateur SharePoint Farm (autorisations complètes)	Compte de domaine doté d'autorisations administrateur complètes pour tous les serveurs Windows et les services au niveau de la batterie dans la batterie de serveurs SharePoint. Ce compte doit être spécifié lors de l'installation de McAfee Security for Microsoft SharePoint.
Administrateur SharePoint (autorisations complètes)	Compte de domaine doté d'autorisations administrateur complètes pour SharePoint installé sur un serveur unique. Ce compte doit être spécifié lors de l'installation de McAfee Security for Microsoft SharePoint.
Utilisateur personnalisé (autorisations minimales)	Compte de domaine doté d'autorisations minimales/privilèges de base requis pour l'exécution du produit. Ce compte doit être spécifié lors de l'installation de McAfee Security for Microsoft SharePoint. Consultez les instructions de la section <i>Création d'un compte d'utilisateur de domaine personnalisé avec les autorisations SQL minimales</i> .
Administrateur Windows	Compte qui est membre du groupe d'administrateur local permettant de lancer le programme d'installation de McAfee Security for Microsoft SharePoint. Il peut s'agir du même compte d'administrateur de batterie en cas d'utilisation pour l'installation du produit. Cependant, si l'utilisateur personnalisé sert à exécuter McAfee Security for Microsoft SharePoint, vous devez disposer d'un compte d'administrateur Windows pour exécuter le programme d'installation.
Administrateur ePolicy Orchestrator	Permet de déployer, gérer et administrer McAfee Security for Microsoft SharePoint à partir d'un serveur ePolicy Orchestrator.

Configuration système requise

Avant d'installer le produit, assurez-vous que votre système client est prêt et qu'il est conforme à la configuration requise.

Installation de SharePoint en mode serveur unique

Quand le serveur SharePoint est installé en mode serveur unique, voici une liste d'instructions à appliquer avant de procéder à l'installation de McAfee Security for Microsoft SharePoint.

- Assurez-vous de disposer des informations d'identification d'administrateur Windows afin de pouvoir installer McAfee Security for Microsoft SharePoint. Ce compte doit être membre du groupe d'administrateurs Windows et les informations d'identification sont requises pour lancer le programme d'installation du produit.
- Assurez-vous de disposer des informations d'identification administrateur SharePoint pour les fournir au programme d'installation de McAfee Security for Microsoft SharePoint. Ce compte doit être membre du groupe d'administrateurs locaux sur le serveur SharePoint et le serveur de base de données pour l'accès à la base de données distante.
- Si vous effectuez une mise à niveau depuis une version précédente, désinstallez toutes les éventuelles versions antérieures du produit autres que McAfee Security for Microsoft SharePoint 2.5 Correctif 1.
- Choisissez un port ouvert/non utilisé sur le serveur où vous voulez héberger le site du logiciel. Vous pouvez utiliser le port par défaut (45900), s'il est disponible. Utilisez Telnet sur un port via l'invite de commande Windows pour vérifier s'il est ouvert.

A partir d'un serveur distant, utilisez la commande telnet <nom hôte ou adresse IP> <Port>.



- En cas de connexion refusée, le port n'est pas disponible (ouvert).
- Si la connexion est acceptée, le port est utilisé et n'est pas disponible.
- En cas de délai d'expiration, un pare-feu bloque l'accès. A partir du même serveur, utilisez `netstat -an` pour vérifier si le port 45900 est à l'écoute.

Installation de SharePoint dans une batterie

Voici les actions que vous devez effectuer avant d'installer McAfee Security for Microsoft SharePoint quand le serveur SharePoint est installé dans une batterie.

McAfee vous recommande d'installer McAfee Security for Microsoft SharePoint avec les informations d'identification de l'administrateur de la batterie de serveurs SharePoint. Le logiciel doit être installé sur les serveurs suivants de la batterie de serveurs :

- Tous les serveurs Web Front-End (WFE) qui hébergent des sites de portail.
- Tous les serveurs WFE qui hébergent des sites d'équipes WSS (Windows SharePoint Services).
- Quand un serveur WFE dirige le trafic vers un autre rôle SharePoint dans la batterie, McAfee Security for Microsoft SharePoint doit être installé à la fois sur le serveur WFE et le rôle SharePoint de destination. Ceci est dû au fait que le trafic redirigé ne passe pas par McAfee Security for Microsoft SharePoint sur le WFE.

McAfee Security for Microsoft SharePoint n'est pas requis sur les types de serveurs ci-dessous :

- Serveurs d'applications



Lorsque vous configurez des analyses à la demande ou planifiées dans un environnement où McAfee Security for Microsoft SharePoint n'est pas installé sur des serveurs d'applications, tout le contenu de la base de données est récupéré à partir des serveurs d'applications et diffusé sur le réseau à destination de WFE pour analyse. En pareils cas, il peut être pratique d'installer McAfee Security for Microsoft SharePoint localement sur les serveurs d'applications afin de réduire au minimum l'utilisation de la bande passante.

- Serveurs de recherche
- Serveurs de gestion d'index



Si vous choisissez d'installer McAfee Security for Microsoft SharePoint sur un serveur d'indexation, veuillez à planifier l'indexation en dehors des heures de pointe afin de limiter l'impact de l'analyse à l'accès sur les performances du serveur.

- Serveurs de travaux
- Serveurs Microsoft SQL Server

Si la stratégie de votre organisation vous empêche d'utiliser les informations d'identification d'administrateur de la batterie SharePoint ou si vous ne voulez pas les utiliser pour d'autres raisons, vous pouvez créer un compte d'utilisateur de domaine normal personnalisé avec des autorisations minimales nécessaires pour exécuter McAfee Security for Microsoft SharePoint. Consultez les instructions de la section *Création d'un compte d'utilisateur de domaine personnalisé avec les autorisations SQL minimales*.

Types d'installation

Il est possible d'installer McAfee Security for Microsoft SharePoint sur un serveur autonome ou de le déployer via ePolicy Orchestrator.

Voir aussi

Intégration avec ePolicy Orchestrator, page 4

Installation standard

Pendant l'installation standard, un assistant s'affiche pour vous accompagner tout au long du processus, par le biais d'une série d'instructions que vous devez suivre.

Procédure

- 1 Pour installer McAfee Security for Microsoft SharePoint, téléchargez l'archive `MSMS30_FR.zip` (pour le français) et procédez à l'extraction des fichiers vers un emplacement temporaire sur votre système.
- 2 Double-cliquez sur `setup.exe`. Si le logiciel est une version sous licence, la boîte de dialogue **Contrat de licence utilisateur final McAfee** s'affiche.
- 3 Dans les menus déroulants, choisissez le type d'expiration de licence et l'endroit où vous avez acheté le logiciel.
- 4 Acceptez les termes de l'accord de licence, puis cliquez sur **OK**.

Pendant l'installation du logiciel, un assistant s'affiche pour vous accompagner tout au long du processus, par le biais d'une série d'instructions que vous devez suivre.

- 5 Cliquez sur **Suivant**.
- 6 McAfee Security for Microsoft SharePoint est installé par défaut sur le port 45900. Désignez un port personnalisé sur lequel Microsoft Internet Information Server doit héberger McAfee Security for Microsoft SharePoint, puis cliquez sur **Suivant**.

La boîte de dialogue **Dossier destinataire** s'affiche.

- 7 Cliquez sur **Suivant** pour installer le logiciel à l'emplacement par défaut C:\Program files (x86).



- Vous pouvez choisir un autre emplacement pour l'installation du logiciel en cliquant sur **Parcourir**. Choisissez un autre emplacement, cliquez sur **OK** pour revenir à l'assistant d'installation, puis cliquez sur **Suivant**.
- La bonne pratique est d'avoir McAfee Security for Microsoft SharePoint installé dans le répertoire par défaut du lecteur système. Cependant, vous pouvez sélectionner un autre emplacement si nécessaire.

La boîte de dialogue **Compte de la base de données** s'affiche.

- 8 Entrez votre nom de compte (domaine ou groupe de travail\pseudo) et votre mot de passe, puis cliquez sur **Suivant**.
- 9 Tapez les informations d'identification du système où SharePoint est installé. Par exemple :
Domaine\pseudo ou Groupe de travail\pseudo.
 - a Les références d'identification de compte sont validées par le serveur. Le compte doit être membre du groupe Administrateurs local sur le serveur sur lequel vous installez McAfee Security for Microsoft SharePoint.



Si les références d'identification d'utilisateur ne peuvent être résolues par le serveur, une boîte de dialogue d'avertissement vous invite à vérifier vos références d'identification.

- b Vérifiez si vous avez saisi les références d'identification correctes. Cliquez sur **OK**, puis sur **Suivant** pour ignorer l'avertissement et poursuivre la procédure d'installation avec des informations de compte non résolues.

La boîte de dialogue **Prêt à installer l'application** s'affiche.



Vous pouvez utiliser `SetSQLAct.exe` pour modifier vos références d'identification en cas de saisie incorrecte lors de l'installation de McAfee Security for Microsoft SharePoint. Cet utilitaire est situé à l'emplacement suivant : <Dossier d'installation>\bin.

A partir de l'invite de commande, tapez `SetSqlAct.exe /USER=<nomutilisateur> /PASSWORD=<motdepasse> /DOMAIN=<domaine>`.

- 10 Cliquez sur **Suivant**. Une barre de progression s'affiche pour indiquer le statut de la procédure d'installation.

- 11 Une fois l'installation terminée, sélectionnez ou désélectionnez les options suivantes selon le cas, puis cliquez sur **Terminer**.
- **Afficher le Readme** — Pour lire les notes de distribution du logiciel qui décrivent les caractéristiques du produit et les modifications de dernière minute à la documentation, et signalent tout comportement connu ou autres problèmes du produit.
 - **Lancer l'interface utilisateur** : pour lancer l'interface utilisateur graphique du logiciel. Ceci lance le produit en mode autonome.
 - **Mettre à jour** — Pour télécharger les dernières mises à jour du produit et vous assurer ainsi d'appliquer les mesures de sécurité les plus actuelles pour lutter contre des menaces en constante évolution. Votre système doit être connecté à Internet pour recevoir les mises à jour automatiques régulièrement.

McAfee Security for Microsoft SharePoint est à présent installé sur votre système.

Mise à niveau à partir d'une version précédente

McAfee Security for Microsoft SharePoint prend en charge la mise à niveau des paramètres de configuration à partir de la version précédente du logiciel.

Lors de la mise à niveau vers une nouvelle version, il est inutile de désinstaller la version existante. Le programme d'installation met à jour votre installation vers la nouvelle version.



La mise à niveau est prise en charge à partir de la version du produit 2.5 Correctif 1 jusqu'à cette version.

Procédure

- 1 En tant qu'administrateur, connectez-vous au système sur lequel Microsoft SharePoint Server est installé.
- 2 Dans le dossier d'installation du fichier d'archive .zip extrait, double-cliquez sur `setup.exe`.
- 3 Dans l'écran **Préparation de l'installation**, l'Assistant d'installation est en cours de préparation et tous les fichiers d'installation nécessaires sont extraits. Le processus est le même qu'avec l'installation standard. Consultez la section *Installation standard*. Une fois le processus terminé, l'écran **Modifications terminées** s'affiche.

Vous avez à présent terminé la mise à niveau vers la dernière version disponible.

Tâches postérieures à l'installation

Après avoir installé McAfee Security for Microsoft SharePoint, il est conseillé de le tester.

Test de votre installation

Une fois l'installation de McAfee Security for Microsoft SharePoint terminée, il est recommandé de la tester afin de s'assurer que le logiciel est installé correctement.

Pour vérifier si le logiciel McAfee Security for Microsoft SharePoint installé est opérationnel, exécutez le fichier test antivirus standard *EICAR* sur l'ordinateur sur lequel le logiciel a été installé.



Ce fichier a été conçu en commun par divers éditeurs d'antivirus du monde entier désireux de créer un standard unique auquel les clients puissent se référer pour déterminer l'efficacité d'un antivirus.

Test de l'analyseur à l'accès

Vous pouvez tester l'analyseur à l'accès en utilisant le fichier EICAR.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Lancez le serveur Microsoft SharePoint.
- 2 Copiez la ligne suivante dans un fichier, puis enregistrez le fichier sous le nom `EICAR.TXT` :
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
La taille du fichier est de 68 ou 70 octets.



Si tout autre logiciel de sécurité est installé sur votre serveur (par exemple McAfee VirusScan Enterprise), vous devez désactiver son analyseur pendant cette opération. Ceci vise à empêcher le fichier d'être identifié par un autre logiciel de sécurité.

- 3 Démarrez le logiciel McAfee Security for Microsoft SharePoint et ajoutez le fichier `EICAR.TXT` à votre serveur Microsoft SharePoint Server. L'action de l'analyseur à l'accès de McAfee Security for Microsoft SharePoint étant configurée pour **empêcher le chargement/téléchargement de l'élément**, le fichier n'est donc pas enregistré sur votre serveur SharePoint.

Test de l'analyseur à la demande

Vous pouvez tester l'analyseur à la demande en utilisant le fichier `EICAR.TXT`.

Pour consulter la définition des options, cliquez sur ? dans l'interface.

Procédure

- 1 Lancez l'interface d'administration Microsoft SharePoint en cliquant sur **Démarrer | Programmes | SharePoint Portal Server | Gestion centrale de SharePoint**
- 2 Cliquez sur **Configurer les paramètres d'antivirus** dans **Configuration de la sécurité**.
- 3 Désélectionnez **Analyser les documents au téléchargement** et **Analyser les documents au téléchargement**.
- 4 Effacez du fonds documentaire la copie précédente du fichier `EICAR.TXT`.
- 5 Ajoutez à nouveau le fichier `EICAR.TXT` au fonds documentaire. Planifiez une analyse à la demande de ce fonds documentaire. Le logiciel McAfee Security for Microsoft SharePoint signale avoir détecté le fichier test EICAR, conformément au paramètre de stratégie à la demande par défaut **Remplacer l'élément par une alerte**.
- 6 Une fois que vous avez fini de tester votre installation, supprimez ce fichier pour éviter d'alerter les utilisateurs non informés.
- 7 Assurez-vous de réactiver l'analyse à l'accès pour fournir une protection en temps réel à votre ordinateur SharePoint contre les virus et les fichiers et contenu indésirables.



Si vous avez désactivé tout autre logiciel antivirus pendant ces tests, prenez soin de le réactiver.

Composants et services installés

Le logiciel installe ces composants sur votre serveur SharePoint.

Pour accéder à ces composants, cliquez sur **Démarrer | Programmes | McAfee | McAfee Security for Microsoft SharePoint**, puis sélectionnez le composant :

- **Editeur de liste de sites McAfee AutoUpdate** — Spécifie l'emplacement à partir duquel les mises à jour automatiques (y compris les fichiers DAT et les moteurs d'analyse) sont téléchargées.
- **MSMS (interface utilisateur Mozilla)** — Lance la version autonome du logiciel à l'aide du navigateur Mozilla Firefox.
- **MSMS (interface utilisateur Web)** — Lance la version autonome du logiciel à l'aide du navigateur Web.
- **Contrôle d'accès** — Autorise ou refuse l'accès à l'interface utilisateur de McAfee Security for Microsoft SharePoint à des utilisateurs ou groupes spécifiques.

Services disponibles

- **McAfee Framework Service** : préalable à l'installation et à l'utilisation d'ePolicy Orchestrator. Pour plus de détails concernant ce service, consultez la documentation produit d'ePolicy Orchestrator.
- **McAfee Portalshield** : protège votre serveur Microsoft SharePoint Server contre les virus, le contenu indésirable, les programmes potentiellement indésirables et les types de fichier/messages interdits.

3

Tableau de bord

Le tableau de bord présente les informations de manière lisible et facilement compréhensible. Il contient des informations critiques concernant le niveau de protection du serveur contre les virus et les programmes potentiellement indésirables. Il présente également des informations relatives aux statistiques de détection, aux composants supplémentaires installés dans le produit, à la version de ces composants (moteur et fichiers DAT, par exemple), à la licence du produit et aux éléments analysés récemment.

Sommaire

- *Informations statistiques des éléments détectés*
- *Versions et mises à jour du produit*
- *Affichage des éléments analysés récemment*
- *Analyse à la demande*
- *Rapports graphiques*

Informations statistiques des éléments détectés

Affiche des informations détaillées sur le nombre total d'éléments analysés par McAfee Security for Microsoft SharePoint, et le nombre d'éléments ayant déclenché la détection et étant mis en quarantaine en fonction de la catégorie de détection. Le tableau de bord fournit également ces informations statistiques sous la forme d'un graphique, pour en faciliter l'interprétation, et surveille les taux de détection.

Les **Statistiques** comprennent les sections suivantes :

- Paramètres à l'accès
- Détections
- Analyse
- Graphique

Paramètres à l'accès : spécifie si vous voulez analyser les documents lors d'une opération de chargement ou de téléchargement. Ce paramètre est lié aux paramètres d'administration centrale antivirus de SharePoint. Nous vous recommandons de toujours activer les **Paramètres à l'accès**.



Le fait de cliquer sur **Réinitialiser** efface les informations statistiques de tous les compteurs dans la section **Détections** et réinitialise leur valeur à zéro. La réinitialisation des statistiques n'entraîne pas la suppression des éléments mis en quarantaine sous **Éléments détectés**. Ces compteurs dépendent du chemin d'accès à la base de données. Par conséquent, si vous modifiez ce chemin d'accès sous **Paramètres et diagnostics | Éléments détectés | Base de données locale**, les compteurs seront remis à zéro.

Pour modifier les paramètres du tableau de bord tels que la fréquence d'actualisation, le nombre maximal d'éléments figurant sous **Éléments récemment analysés**, les unités de l'échelle du graphique, les paramètres des graphiques et diagrammes (par ex., graphique à secteurs en 3D ou décomposé, transparence), accédez à **Paramètres et diagnostics** | **Préférences de l'interface utilisateur**.

Détections

Affiche l'ensemble des informations statistiques relatives au nombre d'éléments analysés par McAfee Security for Microsoft SharePoint et définis comme non infectés ainsi que celles se rapportant au nombre d'éléments ayant déclenché une détection. Le compteur approprié est incrémenté selon la catégorie de détection.

Les valeurs fournies correspondent au nombre d'éléments qui déclenchent l'une des méthodes de détection.



Si votre serveur McAfee Security for Microsoft SharePoint est géré par ePO et que vous redémarrez le service ou cliquez sur le bouton **Réinitialiser**, ces statistiques varient dans les rapports ePO en fonction des données d'historique stockées dans ePO. Pour plus d'informations sur les rapports ePO, consultez le chapitre *Intégration McAfee Security for Microsoft SharePoint avec ePolicy Orchestrator*.

Tableau 3-1 Icônes utilisées dans la section Détections

Icône	Description
	Fournit des informations supplémentaires sur la catégorie de détection lorsque vous placez le pointeur de la souris dessus.
	Indique que les statistiques de la catégorie de détection concernée apparaissent dans le graphique.
	Indique que les statistiques de la catégorie de détection concernée n'apparaissent pas dans le graphique.

Le tableau suivant fournit d'autres informations sur les différentes catégories de détection.

Tableau 3-2 Définition des catégories de détection




Catégorie	Informations supplémentaires	Description
Non infecté	<p>S'il y a davantage d'éléments non infectés que les détections, l'activation de l'icône  pour les éléments non infectés peut supprimer le graphique d'autres catégories. Dans ce type de scénario, désactivez l'icône  en regard de la catégorie Non infecté.</p> 	Désigne les éléments légitimes ne représentant aucune menace pour l'utilisateur et ne déclenchant aucun des analyseurs.
Virus		Fichier de programme informatique capable de se joindre à des disques ou à d'autres fichiers et de se répliquer à l'infini, généralement à l'insu de l'utilisateur et sans son autorisation. Certains virus se joignent à des fichiers, de sorte qu'au moment de l'exécution du fichier infecté, le virus s'exécute également. D'autres virus se logent dans la mémoire d'un ordinateur et infectent les fichiers à mesure que l'ordinateur en ouvre, en modifie ou en crée de nouveaux. Certains virus présentent des symptômes, d'autres endommagent les fichiers et les systèmes informatiques, mais aucun de ces éléments n'est essentiel à la définition d'un virus ; un virus n'occasionnant pas de dommages demeure un virus.
	Virus détecté	Nombre de virus détectés dans un élément.
	Virus nettoyé	Nombre de virus nettoyés dans un élément.
Programmes potentiellement non désirables		Les programmes potentiellement indésirables (PUP) désignent des programmes logiciels écrits par des entreprises légitimes, qui peuvent nuire aux stratégies de sécurité ou de confidentialité d'un ordinateur sur lequel ils ont été installés par inadvertance. Ces programmes peuvent avoir été téléchargés avec une application légitime dont vous avez besoin.
	Programme potentiellement indésirable détecté	Nombre de programmes potentiellement indésirables détectés dans un élément.
	Programme potentiellement indésirable bloqué	Nombre de programmes potentiellement indésirables bloqués à partir d'un élément.
Messages/types de fichiers interdits		Certains types de pièce jointe sont susceptibles d'être des virus.
	Types de fichiers interdits	Nombre de types de fichier interdits détectés dans un élément.
	Messages interdits	Nombre de messages interdits détectés dans un élément.

Tableau 3-2 Définition des catégories de détection (suite)


Catégorie	Informations supplémentaires	Description
Conformité et DLP	 Pour afficher les dictionnaires disponibles, cliquez sur la liste déroulante Catégorie à partir de Gestionnaire de stratégies Ressource partagée Dictionnaires de conformité et DLP.	<p>Le logiciel offre une fonctionnalité d'analyse de contenu de référence. Résultat : un contrôle très strict du contenu confidentiel sous quelque forme que ce soit en vue de favoriser la conformité à de nombreuses réglementations locales, nationales et internationales en vigueur.</p> <p>Favorisez la prévention des fuites de données en utilisant Data Loss Prevention (DLP), la solution de protection la plus étendue du secteur, qui assure la comparaison de formes en vue de détecter des données et la gestion des messages basés sur des stratégies afin de prévenir la fuite de données sortantes.</p>
	Conformité et DLP	Nombre de détections de conformité et DLP dans un élément.
Contenu non désirable		Un contenu indésirable désigne tout contenu que l'utilisateur ne souhaite pas voir sur le serveur. Il est possible de définir les règles au moyen de certains mots ou expressions qui déclenchent ensuite une stratégie correspondante et bloquent le document.
	Packers	Un fichier exécutable compressé se décompresse et/ou se déchiffre dans la mémoire pendant qu'il est en cours d'exécution, de sorte que le fichier situé sur le disque ne ressemble jamais à son image mémoire. Les programmes de compression (« packers ») sont spécialement conçus pour contourner les logiciels de sécurité et éviter l'ingénierie inverse.
	Contenu crypté/corrompu	Documents qui sont classés comme comportant un contenu chiffré ou corrompu.
	Contenu crypté	Le contenu de certains documents peut être crypté, ce qui signifie qu'il est impossible à analyser.
	Contenu signé	<p>Lorsque vous envoyez des informations par voie électronique, elles risquent d'être altérées, accidentellement ou délibérément.</p> <p>Si le message comporte un virus ou du contenu indésirable, ou s'il est trop volumineux, il est possible que le logiciel en nettoie ou en supprime certaines parties. Le document demeure valide, et lisible, mais la signature numérique d'origine est cassée. Vous ne pouvez vous fier au contenu du document car il a peut-être été également altéré d'autres manières.</p> <p>Les stratégies de gestion du contenu signé spécifient de quelle manière les documents munis de signatures numériques doivent être traités.</p>
	Contenu corrompu	Le contenu de certains fichiers peut être corrompu et, par conséquent, il ne peut pas être analysé.

Tableau 3-2 Définition des catégories de détection (suite)

Catégorie	Informations supplémentaires	Description
	Déni de service	Moyen d'attaque utilisé contre un ordinateur, un serveur ou un réseau. L'attaque est une conséquence intentionnelle ou accidentelle du code d'instruction qui est lancé soit depuis un réseau distinct ou un système connecté à Internet, soit directement depuis l'hôte. L'attaque vise à désactiver ou arrêter la cible, et perturbe la capacité du système à répondre à des demandes de connexion légitimes. Une attaque par déni de service submerge sa cible de fausses demandes de connexion de sorte que la cible ignore les demandes légitimes.
	Contenu protégé	Le contenu de certains fichiers est protégé et, par conséquent, il ne peut pas être analysé.
	Fichiers protégés par mot de passe	Le contenu de certains fichiers est protégé par mot de passe. Il n'est pas possible d'analyser les fichiers protégés par mot de passe.
	Messages MIME incomplets	MIME est l'acronyme de Multipurpose Internet Mail Extensions. Il s'agit d'un standard de communication qui permet de transférer des formats non-ASCII via des protocoles, tels que SMTP, ne prenant en charge que les caractères ASCII 7 bits. MIME définit différentes façons de coder les formats non-ASCII afin qu'ils puissent être représentés à l'aide du jeu de caractères ASCII à 7 bits.
	Autres	Toutes les autres détections qui ne sont pas classées dans les catégories de détection spécifiées.

Analyse

Affiche des informations sur le nombre total d'éléments analysés par McAfee Security for Microsoft SharePoint ainsi que la durée moyenne d'analyse de tous les éléments depuis la dernière réinitialisation.

Tableau 3-3 Définition des options

Option	Définition
Durée moyenne de l'analyse (en ms)	Indique la durée moyenne que met McAfee Security for Microsoft SharePoint pour analyser tous les éléments qui atteignent le serveur SharePoint. Pour comprendre le mode de calcul utilisé, considérons l'exemple suivant où : <ul style="list-style-type: none"> • T = durée totale de l'analyse de tous les éléments depuis le dernier redémarrage du service McAfee PortalShield. • N = nombre total d'éléments analysés depuis le dernier redémarrage du service McAfee portalShield. Dans ce cas, la durée moyenne de l'analyse = T/N (en millisecondes)
Nombre total d'éléments analysés	Indique le nombre total d'éléments analysés depuis la dernière réinitialisation des compteurs de statistiques.

Graphique

Affiche dans un format graphique les statistiques relatives aux détections analysées par le logiciel.

Tableau 3-4 Icônes utilisées dans la section Graphique



Icône	Description
	Affichez les informations statistiques des compteurs sélectionnés sous forme de graphique à barres. Cette fonctionnalité s'avère pratique pour obtenir des statistiques sur le nombre total d'éléments analysés et les éléments ayant déclenché une détection lors de la période sélectionnée.
	Affichez les informations statistiques des compteurs sélectionnés sous forme de graphique à secteurs. Cette fonctionnalité s'avère pratique pour obtenir le pourcentage d'éléments analysés et les éléments ayant déclenché une détection lors de la période sélectionnée.

Tableau 3-5 Définition des options

Option	Définition
Graphique	<ul style="list-style-type: none"> • Non infecté : affiche des informations sur le nombre d'éléments qui étaient non infectés pour la plage horaire considérée. • Virus : affiche des informations sur le nombre d'éléments qui ont été détectés comme virus par le logiciel pour la plage horaire considérée. • Contenu indésirable : affiche des informations sur le nombre d'éléments qui ont été détectés comme contenu indésirable par le logiciel pour la plage horaire considérée. • Programmes potentiellement indésirables : affiche des informations sur le nombre d'éléments qui ont été détectés comme programmes potentiellement indésirables par le logiciel pour la plage horaire considérée. • Messages/types de fichiers interdits : affiche des informations sur le nombre d'éléments qui ont été détectés comme messages/types de fichiers interdits par le logiciel pour la plage horaire considérée. • Conformité et DLP : affiche des informations sur le nombre d'éléments qui ont été détectés comme étant de type Conformité et DLP par le logiciel pour la plage horaire considérée.
Agrandir le graphique	Permet de spécifier le pourcentage d'agrandissement du graphique Détections . Cette option vous permet d'afficher une vue agrandie du graphique, ce qui s'avère pratique lorsque le graphique par défaut visible dans le tableau de bord est de plus en plus encombré d'informations et devient illisible dans la fenêtre de navigateur active.
Plage horaire	Permet de spécifier la période pour laquelle vous souhaitez consulter les statistiques. Les options disponibles sont les suivantes : <ul style="list-style-type: none"> • Dernières 24 heures • Derniers 7 jours • Derniers 30 jours

Versions et mises à jour du produit

Cette section présente des informations importantes concernant l'état des fichiers DAT et des pilotes installés sur le logiciel, et indique si les versions les plus récentes sont présentes. Elle fournit également des informations sur le type de licence du produit.

Versions et mises à jour




La section **Versions et mises à jour** du **Tableau de bord** propose les onglets suivants :

- Informations de mise à jour
- Informations produit
- Licences

Informations de mise à jour

Cet onglet présente des informations concernant la version des fichiers DAT de l'antivirus et du moteur antivirus, leur statut et la date de leur dernière mise à jour. McAfee Security for Microsoft SharePoint utilise le site Web de mise à jour de McAfee ou fait appel à McAfee ePO pour mettre à jour automatiquement son DAT antivirus, son moteur et ses règles quotidiennement.

Tableau 3-6 Définition des options – Informations de mise à jour

Option	Définition
Dernière mise à jour réussie	Affiche l'heure à laquelle la dernière mise à jour du logiciel a eu lieu.
Mettre à jour maintenant	Permet de mettre immédiatement à jour le produit avec la dernière version du moteur et des pilotes. Cette méthode s'avère pratique lorsqu'une attaque virale vient de se produire et que vous ne pouvez pas attendre que l'heure de mise à jour planifiée du logiciel arrive.  : indique que votre DAT antivirus est à jour.  : indique que votre DAT antivirus n'est pas à jour.
Fréquence des mises à jour	Affiche la fréquence de mise à jour logicielle planifiée.
Modifier la planification	Permet de planifier ou de modifier la mise à jour logicielle du produit. Pour plus d'informations sur la procédure de mise à jour du logiciel, consultez la section <i>Planification d'une mise à jour logicielle</i> .
Afficher le statut	Permet d'afficher le statut actuel de la tâche de mise à jour : heure de début, durée d'exécution, statut actif, progression de la tâche, etc.  Vous pouvez consulter le statut de la mise à jour actuelle. Pour consulter le statut des précédentes mises à jour : Paramètres et diagnostics Journal du produit .
Moteur antivirus Version du DAT Pilotes supplémentaires	Affiche les informations les plus récentes concernant le moteur antivirus, la version des fichiers DAT et les pilotes supplémentaires, ainsi que la date à laquelle elles ont été mises à jour.
Virus détectés par les pilotes supplémentaires	Affiche les éléments détectés par Extra.DAT pour supprimer des virus spécifiques. Les fichiers <code>EXTRA.DAT</code> contiennent des informations dont se sert le logiciel pour détecter un nouveau virus. Lorsqu'un virus important est découvert et qu'une détection supplémentaire s'avère nécessaire, un fichier <code>EXTRA.DAT</code> est mis à disposition jusqu'à ce que la mise à jour du fichier DAT normale soit distribuée.

Planification d'une mise à jour logicielle

Maintenez à jour votre logiciel avec la dernière version des fichiers DAT antivirus et du moteur antivirus en planifiant une mise à jour automatique.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Cliquez sur **Tableau de bord | Statistiques & Informations**.
- 2 Dans la section **Versions et mises à jour**, cliquez sur l'onglet **Informations de mise à jour**.
- 3 Dans **Fréquence des mises à jour**, cliquez sur **Modifier le calendrier**.

La page **Modifier le calendrier** s'affiche.

- 4 A partir de l'onglet **Choisir une heure**, spécifiez le moment auquel vous souhaitez planifier une mise à jour. Les options disponibles sont les suivantes :
 - **Non planifiée** : sélectionnez cette option si vous n'avez pas décidé du moment où vous souhaitez exécuter la tâche de mise à jour.
 - **Une fois** : spécifiez les date et heure auxquelles vous souhaitez planifier l'exécution unique d'une mise à jour.
 - **Heures** : sélectionnez cette option pour planifier la tâche de mise à jour selon le nombre d'heures spécifié.
 - **Jours** : sélectionnez cette option pour planifier la tâche de mise à jour en fonction du nombre d'exécutions hebdomadaires souhaité.
 - **Semaines** : sélectionnez cette option pour planifier la tâche de mise à jour en fonction du nombre d'exécutions mensuelles souhaité.
 - **Mois** : sélectionnez cette option pour planifier la tâche de mise à jour en fonction du nombre d'exécutions annuelles souhaité.



- Une mise à jour quotidienne est planifiée par défaut. McAfee recommande de ne pas modifier la valeur par défaut.
- Si le serveur est managé à l'aide de McAfee ePO, les paramètres définis dans McAfee ePO sont prioritaires par rapport aux paramètres locaux.

- 5 Cliquez sur **Enregistrer**, puis sur **Appliquer**.

Vous avez à présent terminé la planification d'une mise à jour logicielle.

Informations produit

Présente des informations sur le nom du produit, la version, les Service Pack et les HotFix.

Tableau 3-7 Définition des options

Option	Définition
Nom du produit	Spécifie McAfee Security for Microsoft SharePoint comme nom du produit.
Version du produit	Indique la version du produit au format : <Version majeure>.<Version mineure>.<numéro du build>.<numéro du package>. Par exemple - 3.0.1000.100

Tableau 3-7 Définition des options (suite)


Option	Définition
Service Pack	Répertorie les informations sur le Service Pack ou le patch (le cas échéant).
Hotfixes	Dresse la liste des HotFix et des correctifs installés.

Licences

Les licences contiennent des informations sur le type de licence installé, la date d'expiration et les jours restants avant l'expiration du produit et des composants installés.

Tableau 3-8 Définition des options

Option	Définition
Description	Spécifie le nom du produit installé.
Type	Indique si le produit installé correspond à une version de type Sous licence ou Evaluation .
Expire	S'affiche lorsqu'une version d' Evaluation du logiciel est installée. Indique les date et heure d'expiration de la licence.
Nombre de jours avant l'expiration	S'affiche lorsqu'une version d' Evaluation du logiciel est installée. Indique le nombre de jours restant avant l'expiration du produit.

 Pour une mise à niveau d'une version d'évaluation vers une version sous licence du produit, contactez le support McAfee.

Affichage des éléments analysés récemment

Le tableau de bord vous permet d'afficher une vue d'ensemble des éléments analysés récemment.

La section **Éléments récemment analysés** vous offre des informations d'exécution sur tous les éléments analysés par le produit. Par défaut, seuls 10 éléments figurent sous la section **Éléments récemment analysés**. Cependant, vous pouvez afficher jusqu'à 100 éléments en modifiant l'option **Nombre maximal d'éléments analysés récemment** sous **Paramètres et diagnostics | Préférences de l'interface utilisateur | Paramètres du tableau de bord | Paramètres des rapports**.



Les éléments figurant dans la section **Éléments récemment analysés** seront effacés si vous redémarrez le service **McAfee Portalshield** à partir de la console **Services**.

Tableau 3-9 Définition des options

Option	Définition
Date/Heure	Date et heure de l'analyse la plus récente.
Nom du fichier	Nom du fichier analysé.
Nom de la détection	Nom de la détection. Par exemple, le nom d'un virus.
Dossier	Emplacement du fichier analysé dans Sharepoint.
Nom d'utilisateur	Nom de l'utilisateur ayant géré le fichier.
Direction	Direction de la tâche. Par exemple, chargement ou téléchargement.
Mesure prise	Quelle action a été entreprise sur les éléments analysés.
Analysé par	Paramètre de stratégie utilisé pour analyser des éléments. Par exemple, à la demande ou à l'accès.

Tableau 3-9 Définition des options (suite)

Option	Définition
Nom de la tâche	Nom de la tâche ayant déclenché une détection. Par exemple, analyse à l'accès.
Nom de la stratégie	Nom de la stratégie ayant déclenché une détection.



Les valeurs **Nom d'utilisateur**, **Direction**, **Action entreprise** et **Analysé par** sont disponibles uniquement si vous utilisez SharePoint 2010 ou version ultérieure.



: indique que l'élément est sain.



: indique que l'élément a déclenché l'un des analyseurs ou des filtres.



Passez le curseur sur l' pour voir quel analyseur ou filtre a été déclenché. Si l'élément a déclenché plusieurs analyseurs ou filtres, seule la détection dont la priorité est la plus élevée est indiquée.

Analyse à la demande

Un analyseur à la demande est un analyseur de sécurité que vous démarrez manuellement à des heures pratiques ou à intervalle régulier. Il vous permet de définir différentes configurations et d'analyser des dossiers spécifiques.

Le logiciel vous permet de créer des analyses à la demande planifiées. Vous pouvez définir plusieurs planifications, chacune s'exécutant automatiquement à des heures ou à des intervalles prédéfinis.

Situations nécessitant une analyse à la demande

- Il est vivement conseillé de procéder à une analyse à la demande en cas de panne au sein de l'organisation suite à une activité malveillante. Cette tâche permet de garantir que les bases de données Microsoft SharePoint n'ont pas été infectées au cours de la panne ou qu'elles ont été nettoyées.
- McAfee vous conseille d'effectuer une tâche d'analyse à la demande en dehors des heures ouvrables. Lorsqu'une tâche d'analyse à la demande est planifiée au cours d'une heure creuse et qu'elle se poursuit pendant les heures de pointe, vous devez réexaminer les bases de données soumises à l'analyse et définir d'autres planifications en modifiant les données analysées.
- Vous pouvez planifier l'exécution d'une analyse à la demande le week-end afin d'être certain que les bases de données SharePoint ne sont pas infectées et que les anciens fichiers et dossiers sont également analysés par les signatures antivirus les plus récentes.

Raisons justifiant une analyse à la demande

Effectuez une analyse à la demande pour les raisons suivantes :

- Contrôler un ou plusieurs fichiers chargés ou publiés.
- Vérifier que les dossiers dans votre serveur SharePoint sont sains, après la mise à jour des fichiers DAT, afin de détecter d'éventuels nouveaux virus.
- Vérifier que votre ordinateur est complètement propre après avoir détecté et nettoyé un virus.
- Vérifier les fichiers et les dossiers qui se trouvaient sur votre serveur SharePoint, avant l'installation de McAfee Security for Microsoft SharePoint.
- Vérifier les fichiers et les dossiers que vous n'avez pas inclus dans l'analyse à l'accès.

Raisons justifiant une analyse incrémentielles et avec reprise

Après avoir installé McAfee Security for Microsoft SharePoint, exécutez une analyse à la demande complète la première fois. Plus tard, vous pouvez utiliser l'analyse incrémentielle pour analyser uniquement les éléments nouveaux ou modifiés sur votre serveur SharePoint plutôt que d'effectuer une nouvelle analyse de l'ensemble du serveur.

Dans le cas d'une base de données ou d'un serveur plus volumineux, utilisez l'analyse avec reprise. Dans le cas de l'analyse à la demande avec reprise, si une analyse en cours est suspendue, McAfee Security for Microsoft SharePoint enregistre l'état actuel de la tâche d'analyse. Dès que la même tâche est lancée plus tard, l'analyse reprend à partir du dernier dossier analysé. En cas de mise à jour de signature alors qu'une analyse est en pause, le logiciel comporte une option permettant de relancer l'analyse avec les fichiers DAT mis à jour.

Meilleures pratiques pour configurer une stratégie à la demande

- Veillez à toujours activer l'analyseur antivirus, la conformité et DLP et les analyseurs de filtrage de fichiers pour la stratégie à la demande. Pour la véritable détection de type de fichier dans le filtrage de fichier, activez conformité et DLP.
- Sélectionnez l'option **Protection élevée** pour maximiser le niveau de protection de l'analyseur antivirus.
- Choisissez l'option de **Quarantaine** toujours afin de pouvoir récupérer les fichiers de la base de données de quarantaine ultérieurement en cas de besoin.
- Si la taille de la base de données SharePoint est en Go, veillez à répartir votre référentiel SharePoint (applications web, collections de sites, sites, dossiers) dans plusieurs tâches à la demande pour de meilleures performances.
- Si McAfee Security for Microsoft SharePoint est installé dans une configuration de batterie de serveurs SharePoint, distribuez votre référentiel sur plusieurs nœuds.

Par exemple, dans une batterie si vous avez 4 applications Web dans votre serveur SharePoint et 4 nœuds où le produit est installé, vous pouvez répartir la tâche à la demande dans ces 4 nœuds du produit.

- L'installation 1 de McAfee Security for Microsoft SharePoint peut avoir une tâche à la demande créée pour l'application web 1.
- L'installation 2 de McAfee Security for Microsoft SharePoint peut avoir une tâche à la demande créée pour l'application web 2.
- L'installation 3 de McAfee Security for Microsoft SharePoint peut avoir une tâche à la demande créée pour l'application web 3.
- L'installation 4 de McAfee Security for Microsoft SharePoint peut avoir une tâche à la demande créée pour l'application web 4.



Dans une batterie SharePoint, chaque tâche McAfee Security for Microsoft SharePoint **A la demande** affiche le référentiel SharePoint entier.


- Assurez-vous d'exclure l'extension de fichier spécifique SharePoint lors de la configuration de la tâche à la demande. Par défaut, ces extensions de fichiers ne sont pas incluses dans l'analyse à la demande.

Affichage de tâches d'analyse à la demande

Affichez une liste des tâches d'analyse à la demande configurées pour McAfee Security for Microsoft SharePoint.

Affichez les tâches d'analyse à la demande à partir de **Tableau de bord | Analyses à la demande**.


Tableau 3-10 Définition des options

Option	Définition
Nom	Indique le nom de la tâche d'analyse à la demande.
Statut	Indique le statut actuel de la tâche d'analyse à la demande. Le statut peut être le suivant : <ul style="list-style-type: none"> • Inactif • En cours d'exécution • Arrêté • Terminée
Dernière exécution	Indique les date et heure auxquelles la tâche d'analyse à la demande a été exécutée pour la dernière fois.
Prochaine exécution	Indique les date et heure auxquelles la prochaine exécution de la tâche d'analyse à la demande est planifiée.
Action	Affiche la liste des options suivantes pour toutes les tâches d'analyse à la demande disponibles : <ul style="list-style-type: none"> • Modifier • Supprimer • Exécuter maintenant • Afficher le statut • Arrêter <p>L'option Arrêter s'affiche uniquement si une tâche d'analyse à la demande est en cours d'exécution.</p>
Modifier	Permet de modifier les paramètres d'une tâche d'analyse à la demande.
Supprimer	Supprime la tâche d'analyse à la demande sélectionnée.
Exécuter maintenant	Démarre immédiatement la tâche d'analyse à la demande sélectionnée.
Afficher le statut	Affiche l'état actuel d'une tâche d'analyse à la demande. La page Statut de la tâche s'affiche, présentant les onglets suivants : <ul style="list-style-type: none"> • Général : présente des informations supplémentaires sur la tâche d'analyse à la demande telles que la durée totale d'exécution de la tâche, la progression de la tâche, la version du moteur et des fichiers DAT utilisés pour l'analyse, les résultats de l'analyse, le nombre total d'éléments analysés, les règles enfreintes et les dossiers analysés. • Paramètres : présente des informations supplémentaires sur la base de données analysée et la stratégie utilisée. • Détections : fournit des informations sur les détections déclenchées lors de l'analyse. <p> L'option Afficher le statut est uniquement disponible après le démarrage d'une tâche d'analyse à la demande.</p>
Arrêter	Arrête une tâche d'analyse à la demande en cours d'exécution.
Actualiser	Actualise la page en y présentant les informations les plus récentes sur l'analyse à la demande.
Nouvelle analyse	Permet de planifier une nouvelle tâche d'analyse à la demande. Pour plus d'informations sur la procédure de création d'une analyse, consultez la section <i>Création d'une tâche d'analyse à la demande</i> .

Création d'une tâche d'analyse à la demande

Planifiez une tâche d'analyse à la demande pour rechercher ou supprimer des virus et du contenu interdit dans les fichiers et les dossiers.

Procédure

- 1 Cliquez sur **Tableau de bord | Analyses à la demande**. La page **Analyses à la demande** s'affiche.
 - 2 Cliquez sur **Nouvelle analyse**. La page **Planifier une analyse à la demande** s'affiche.
 - 3 A partir de l'onglet **Choisir une heure**, spécifiez le moment auquel vous souhaitez exécuter l'analyse. Les options disponibles sont les suivantes :
 - **Non planifiée** : sélectionnez cette option si vous n'avez pas décidé du moment où vous souhaitez exécuter l'analyse à la demande ou pour désactiver la planification relative à une analyse à la demande existante.
 - **Une fois** : spécifiez les date et heure auxquelles vous souhaitez planifier l'exécution unique d'une analyse à la demande.
 - **Heures** : sélectionnez cette option pour planifier la tâche en fonction des heures, si vous devez exécuter l'analyse à la demande plus d'une fois par jour. Par exemple, en supposant qu'il est 14 h 00 et que vous avez décidé de créer une tâche d'analyse à la demande remplissant les conditions suivantes :
 - l'analyse à la demande doit débuter à 14 h 30 exactement ;
 - l'analyse à la demande doit se produire deux fois par jour.Pour remplir ces conditions, spécifiez 12 pour les heures et 30 pour les minutes.
 - **Jours** : sélectionnez cette option pour planifier la tâche d'analyse en fonction du nombre d'exécutions hebdomadaires souhaité. Par exemple, si l'analyse à la demande doit avoir lieu tous les trois jours, spécifiez 3 sous **jour(s)**, puis sélectionnez l'heure à laquelle la tâche doit démarrer.
 - **Semaines** : sélectionnez cette option pour planifier la tâche d'analyse en fonction du nombre d'exécutions mensuelles souhaité. Par exemple, si l'analyse à la demande doit avoir lieu toutes les deux semaines, spécifiez 3 sous **semaine(s)**, puis sélectionnez les jours et l'heure auxquels la tâche doit démarrer.
 - **Mois** : sélectionnez cette option pour planifier la tâche d'analyse en fonction du nombre d'exécutions annuelles souhaité. Par exemple, si l'analyse à la demande doit avoir lieu le deuxième samedi de chaque mois, sélectionnez **deuxième** dans la liste déroulante **Le**, **Samedi** dans la liste déroulante **de**, puis choisissez les mois concernés et l'heure à laquelle la tâche doit démarrer.
- 
- Activez l'option **Arrêter la tâche si elle s'exécute depuis <n> heure(s) <n> minute(s)** afin d'arrêter une tâche d'analyse à la demande si elle dépasse les heures d'exécution spécifiées.
- 4 Cliquez sur **Suivant**. La page **Choisir les éléments à analyser** s'affiche. Les options disponibles sont les suivantes :
 - **Analyser tous les dossiers** : sélectionnez cette option pour analyser tous les dossiers du serveur SharePoint Server.
 - **Analyser les dossiers sélectionnés** : sélectionnez cette option pour analyser des dossiers spécifiques du serveur SharePoint Server.
 - **Analyser tous les dossiers sauf ceux sélectionnés** : sélectionnez cette option pour analyser tous les dossiers sauf ceux qui ont été ajoutés à la liste **Dossiers à analyser**.

Désélectionnez **Analyser uniquement la bibliothèque de documents** pour analyser toutes les listes figurant dans vos dossiers sélectionnés.

5 Cliquez sur **Suivant**. La page **Planifier une analyse à la demande** s'affiche.

6 Sous l'onglet **Extension(s) des fichiers** : , spécifiez les éventuelles extensions de fichier à exclure de votre analyse à la demande dans **Spécifiez la ou les extensions des fichiers séparées par ','** .



Par défaut, les extensions `thmx`, `aspx`, `asmx`, `css`, `jpg`, `gif`, `htm`, `html`, `png`, `master`, `dwp`, `webpart` et `bmp` sont exclues de l'analyse. Si vous voulez analyser ces fichiers, veuillez à supprimer les extensions requises de cette liste.

7 Sous l'onglet **Avancé** : , spécifiez le type d'analyse.

- Sélectionnez **Désactivé** quand vous ne voulez pas configurer **Analyse avec reprise** ou **Analyse incrémentielle**.
- Sélectionnez **Analyse avec repris** pour activer l'option de reprise d'une analyse à la demande au point où elle a été arrêtée, puis choisissez **Redémarrer l'analyse si le DAT a changé** pour redémarrer une analyse si un fichier DAT a été modifié. Par exemple, si l'analyse à la demande s'arrête après une heure donnée, la reprise de l'analyse relancera la tâche d'analyse à la demande depuis le dossier où le dernier élément a été analysé.
- Sélectionnez **Analyse incrémentielle** pour n'analyser que les fichiers nouvellement ajoutés et non pas tout le référentiel. Sélectionnez l'une des deux options d'analyse incrémentielle.

Option	Définition
Analyser à partir de la date de la dernière analyse	Sélectionnez cette option pour analyser les fichiers nouvellement ajoutés à partir de la dernière date d'analyse. <div data-bbox="641 1075 685 1119" data-label="Image"> </div> La première fois, tous les fichiers sont analysés à partir de la cible sélectionnée. La fois suivante, sont analysés tous les fichiers dont la dernière date de modification est postérieure à la dernière date de fin de cette tâche.
Analyser à partir de la date spécifiée	Sélectionnez cette option pour indiquer une date et une heure pour le début de l'analyse. La valeur par défaut est la date et l'heure du jour.

8 Cliquez sur **Suivant**. La page **Entrer un nom** : s'affiche.

9 Spécifiez un nom évocateur pour la tâche d'analyse à la demande, en fonction de la stratégie sélectionnée à la page précédente. Par exemple, si vous créez une tâche d'analyse à la demande en vue d'effectuer une analyse complète pendant le week-end, choisissez un nom de tâche de type *Analyse complète du week-end*.

10 Cliquez sur **Terminer**, puis sur **Appliquer**.

En suivant ces étapes, vous êtes parvenu au terme de la création d'une tâche d'analyse à la demande.

Rapports graphiques

Générez des rapports graphiques pour comprendre le niveau de menace au cours d'une période spécifique. Ces rapports offrent une vue explicite des éléments détectés sous la forme d'un **Graphique à barres** ou **Graphique à secteurs**.

Ces rapports vous aideront, vous et votre organisation, à identifier les serveurs confrontés aux menaces.

Faites appel aux rapports graphiques pour afficher uniquement le niveau de menace actif, sans entreprendre d'action sur les éléments détectés. Les **Rapports graphiques** vous permettent d'émettre des requêtes basées sur des filtres et d'afficher ainsi les rapports de type **10 principaux** pour différentes détections.

Les **Rapports graphiques** sont classés dans les catégories suivantes :

- **Simple** : options de recherche permettant d'afficher un rapport de type « 10 principaux » pour la journée ou la semaine.
- **Avancé** : comprend d'autres options de recherche permettant d'émettre des requêtes selon divers filtres, plages horaires et options de graphique.

Affichage de rapports graphiques à l'aide de filtres de recherche simples

Générez un rapport graphique sur les détections à l'aide de filtres de recherche de jour ou de semaine simples.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Cliquez sur **Tableau de bord | Rapports graphiques**. La page **Rapports graphiques** s'affiche.
- 2 Cliquez sur l'onglet **Simple**.
- 3 Dans la liste déroulante **Intervalle temporel**, sélectionnez **Aujourd'hui** ou **Cette semaine** pour afficher les éléments détectés qui ont été mis en quarantaine pour le jour ou la semaine spécifié(e).
- 4 Dans la liste déroulante **Filtre**, sélectionnez le rapport à afficher. Les options suivantes sont disponibles :
 - **Classement des 10 premiers virus** : répertorie les 10 principaux noms de virus détectés en les classant d'après leur nombre d'occurrences.
 - **10 principaux programmes indésirables** répertorie les 10 principaux programmes indésirables détectés pouvant constituer des menaces.
 - **Classement des 10 premières détections de contenu indésirable** : répertorie les 10 premières détections de contenu pouvant correspondre à des fichiers protégés par mot de passe ou à un contenu signé.
 - **10 principales détections de conformité et DLP** : répertorie les 10 principales violations de prévention des fuites de données (DLP) et de conformité réglementaire en les classant d'après le nombre de détections ayant déclenché la règle.
 - **Classement des 10 premiers fichiers infectés** : répertorie les 10 principaux noms de fichier détectés en les classant d'après leur nombre d'occurrences.
 - **10 premières détections** : répertorie les 10 principales détections en les classant d'après leur nombre d'occurrences. Ce graphique englobe toutes les catégories : virus, programmes indésirables, conformité et prévention des fuites de données (DLP) et les fichiers infectés répertoriés précédemment.
 - **10 principaux expéditeurs de virus** : répertorie les 10 principaux noms d'utilisateur en les classant d'après leur nombre d'occurrences.
 - **10 principaux expéditeurs de contenu indésirable** : répertorie les 10 principaux noms d'utilisateur en les classant d'après leur nombre d'occurrences.
 - **10 principaux emplacements avec chargements de virus** : répertorie les 10 principaux emplacements de dossiers en les classant d'après leur nombre d'occurrences.

- **10 principaux emplacements avec chargements de contenu indésirable** : répertorie les 10 principaux emplacements de dossiers en les classant d'après leur nombre d'occurrences.
 - **10 principaux expéditeurs d'événements de conformité et DLP** : répertorie les 10 principaux noms d'utilisateur en les classant d'après le nombre de détections ayant déclenché les règles de violations de prévention des fuites de données (DLP) et de conformité.
 - **10 principaux emplacements de conformité et DLP** : répertorie les 10 principaux emplacements de dossiers en les classant d'après le nombre de détections ayant déclenché les règles de violations de prévention des fuites de données (DLP) et de conformité.
 - **10 premières détections de filtres de fichiers** : répertorie les 10 premières détections de filtres de fichiers déclenchées par le système.
 - **10 principaux expéditeurs de filtres de fichiers** : répertorie les 10 principaux noms d'utilisateur en les classant d'après leur nombre d'occurrences.
 - **10 principaux emplacements de filtres de fichiers** : répertorie les 10 principaux emplacements de dossiers en les classant d'après leur nombre d'occurrences.
- 5 Cliquez sur **Rechercher**. Les résultats de la recherche apparaissent dans le volet **Afficher les résultats**.
Dans **Agrandir le graphique**, sélectionnez le pourcentage de zoom vous permettant d'agrandir ou de réduire la vue du graphique dans le volet **Afficher les résultats**.

Affichage de rapports graphiques à l'aide de filtres de recherche avancés

Générez des rapports graphiques sur les détections à l'aide de filtres de recherche avancés.


Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Cliquez sur **Tableau de bord | Rapports graphiques**. La page Rapports graphiques s'affiche.
- 2 Cliquez sur l'onglet **Avancé**.

3 Sélectionnez un, deux ou trois filtres dans la liste :

Tableau 3-11 Filtres principaux

Filtre	Description
Raison	Permet d'effectuer la recherche d'après le déclencheur de détection ou la raison de la mise en quarantaine de l'élément. Quand vous sélectionnez le filtre Raison les filtres secondaires sont activés, ce qui vous permet d'affiner la recherche. Par exemple, vous pouvez très bien rechercher tous les éléments qui ont été mis en quarantaine suite au déclenchement de la règle Filtre de fichiers comme raison.
Numéro de ticket	Permet d'effectuer la recherche d'après le numéro de ticket. Un numéro de ticket est une entrée alphanumérique de 16 chiffres qui est générée automatiquement par le logiciel pour chaque détection.
Nom de la détection	Permet d'effectuer la recherche selon le nom d'un élément détecté.
Analysé par	Permet d'effectuer la recherche selon le type de la tâche. Par exemple, à la demande ou à l'accès.
 Les fonctionnalités répertoriées ci-dessous sont disponibles si vous utilisez Microsoft SharePoint 2010 et versions ultérieures.	
Nom d'utilisateur	Permet d'effectuer une recherche par nom de l'utilisateur dont le fichier a déclenché la détection.
Direction	Permet d'effectuer une recherche par mode d'accès du fichier. Par exemple, Chargement ou Téléchargement.
Dossier	Permet d'effectuer une recherche par dossier SharePoint des fichiers qui ont été mis en quarantaine.
Protection RMS	Permet de rechercher des fichiers qui sont répertoriés comme bénéficiant d'une protection RMS. Le service RMS (Rights Management Service) est un service Microsoft qui permet aux utilisateurs d'empêcher l'accès non autorisé aux documents. Si vous avez un serveur RMS configuré pour protéger vos documents, ces fichiers figureront alors sous Protection RMS.



Un filtre secondaire est disponible pour les filtres **Raison**, **Analysé par** et **Direction**. Si vous préférez ne pas préciser de filtre secondaire, assurez-vous que le filtre est vide ; toutes les détections seront alors recherchées.

Tableau 3-12 Filtres secondaires pour Raison

Filtre	Description
Antivirus	Permet de rechercher des éléments qui ont été détectés quand un virus potentiel a été détecté dans les fichiers.
Conformité et DLP	Permet de rechercher des éléments qui ont été détectés lors du chargement d'un fichier non conforme.
Filtre de fichiers	Permet de rechercher des éléments qui ont été détectés lors du chargement d'une extension de fichier interdite.
Crypté ou corrompu	Permet de rechercher des éléments qui ont été détectés quand un contenu crypté ou corrompu a été détecté dans les fichiers.
Programme potentiellement indésirable	Permet de rechercher des éléments qui ont été détectés quand un un programme potentiellement indésirable a été détecté dans les fichiers.
Packer	Permet de rechercher des éléments qui ont été détectés suite à la détection de programmes de compression (petits programmes, fichiers exécutables compressés ou encore code chiffré) dans les fichiers.

Tableau 3-12 Filtres secondaires pour Raison (suite)

_filtre	Description
Crypté	Permet de rechercher des éléments qui ont été détectés quand un contenu crypté a été détecté dans les fichiers.
Signé	Permet de rechercher des éléments qui ont été détectés quand un contenu signé a été détecté dans les fichiers.
Corrompu	Permet de rechercher des éléments qui ont été détectés quand un contenu corrompu a été détecté dans les fichiers.
Déni de service	Permet de rechercher des éléments qui ont été détectés suite à la survenue d'une menace par déni de service.
Contenu protégé	Permet de rechercher des éléments qui ont été détectés lorsqu'un contenu protégé a été détecté et qu'il n'est pas nécessairement accessible pour examen.
Protégé par mot de passe	Permet de rechercher des éléments qui ont été détectés lorsqu'un contenu protégé par mot de passe a été détecté et qu'il n'est pas nécessairement accessible pour examen.
Sur échec d'analyse	Permet de rechercher les éléments qui n'ont pas pu être scannés.

Tableau 3-13 Filtres secondaires pour Analysé par

_filtre	Description
A la demande	Permet de rechercher des éléments qui ont été détectés par l'analyse à la demande.
A L'ACCES (API WSS VS)	Permet de rechercher des éléments qui ont été détectés par l'analyse à l'accès.

Tableau 3-14 Filtres secondaires pour Direction

_filtre	Description
Téléchargement	Permet de rechercher les éléments ayant déclenché la détection lorsque des éléments ont été chargés vers le serveur SharePoint.
Télécharger	Permet de rechercher les éléments ayant déclenché la détection lorsque des éléments ont été téléchargés à partir du serveur SharePoint.

- 4 Sélectionnez **Toutes les dates** ou une **Plage de dates** dans les listes déroulantes.

Si vous sélectionnez **Toutes les dates**, la requête renvoie les résultats de la recherche provenant de la base de données de quarantaine à compter du premier jour de mise en quarantaine des éventuelles détections. Si vous sélectionnez **Plage de dates**, sélectionnez **Date**, **Mois**, **Année**, **Heure** et **Minutes** dans les champs **De** et **A** afin d'activer votre requête de recherche dans la plage de dates spécifiée.

- 5 Sélectionnez **Graphique à barres** ou **Graphique à secteurs** comme indiqué.
- 6 Si vous sélectionnez **Graphique à secteurs**, choisissez un filtre dans la liste déroulante afin d'affiner la recherche :

Tableau 3-15 Options d'objet de la requête

_filtre	Description
Nom du fichier	Recherche d'après le nom d'un fichier mis en quarantaine.
Nom de la détection	Permet d'effectuer un tri d'après le nom d'un élément détecté.
Raison	Permet d'effectuer un tri d'après le déclencheur de détection ou la raison de la mise en quarantaine de l'élément.
Nom de la règle	Permet d'effectuer un tri d'après le nom de la règle ayant déclenché la détection.

Tableau 3-15 Options d'objet de la requête (suite)

Filtre	Description
Nom de la stratégie	Permet d'effectuer un tri d'après le nom de la stratégie ayant déclenché une détection.
Analysé par	Permet d'effectuer un tri d'après le nom de l'analyse.
Nom d'utilisateur	Permet d'effectuer un tri par nom de l'utilisateur dont les fichiers ont déclenché la détection.
Direction	Permet d'effectuer un tri d'après la direction du fichier.
Dossier	Permet d'effectuer un tri d'après le dossier des fichiers qui ont été mis en quarantaine.

- a Dans **Nombre maximal de résultats**, spécifiez le nombre de résultats de la recherche à afficher. Vous pouvez visualiser un maximum de 99 résultats de la recherche ; ce champ est uniquement disponible pour l'option Graphique à secteurs.
- 7 Cliquez sur **Rechercher**. Les résultats de la recherche apparaissent dans le volet **Afficher les résultats**. Sous **Agrandir le graphique**, sélectionnez le pourcentage de zoom selon lequel vous souhaitez agrandir ou réduire la vue du graphique dans le volet **Afficher les résultats**. Les résultats de la recherche figurent dans le volet **Afficher les résultats**.

Vous avez à présent terminé la génération de rapports graphiques des détections.

4

Éléments détectés

Affichez des informations relatives à tous les éléments contenant des menaces potentielles qui sont détectés et mis en quarantaine par McAfee Security for Microsoft SharePoint. Les différents filtres de recherche mis à votre disposition vous permettent d'affiner vos recherches, d'identifier les éléments mis en quarantaine qui vous intéressent, d'afficher les résultats et de prendre les actions nécessaires concernant ces éléments mis en quarantaine.

Sommaire

- ▶ *Filtres de recherche principaux*
- ▶ *Options de recherche supplémentaires*
- ▶ *Recherche parmi les éléments détectés*
- ▶ *Actions pouvant être entreprises concernant les éléments mis en quarantaine*

Filtres de recherche principaux

Les filtres de recherche permettent de définir les critères de recherche et de lancer des recherches plus efficaces et performantes depuis la base de données de quarantaine.

Ces filtres de recherche figurent dans la section **Afficher les résultats** de la catégorie d'éléments détectés.



L'option **Colonnes à afficher** disponible dans la section **Afficher les résultats** permet de sélectionner les filtres de recherche à visualiser.

Tableau 4-1 Éléments détectés – Filtres de recherche principaux

Filtre de recherche	Définition
Nom du fichier	Permet d'effectuer une recherche d'après le nom du fichier détecté dans l'élément mis en quarantaine. Pour afficher le Nom du fichier utilisé, accédez à Gestionnaire de stratégies Ressource partagée Dictionnaires de conformité et DLP Règles de filtrage des fichiers .
Action entreprise	Permet de rechercher un élément en fonction de l'action entreprise associée. Par exemple, Empêcher le chargement/téléchargement de l'élément ou Autoriser
Nom d'utilisateur	Permet de rechercher un élément d'après l'utilisateur dont les actions ont déclenché la détection.
Dossier	Permet d'effectuer une recherche selon le dossier dans lequel les éléments mis en quarantaine sont enregistrés.
Direction	Permet d'effectuer une recherche d'après la direction du fichier. Par exemple, Chargement ou Téléchargement .

Tableau 4-1 Éléments détectés – Filtres de recherche principaux (suite)

Filtre de recherche	Définition
Protection RMS	Permet d'effectuer une recherche des fichiers bénéficiant d'une protection RMS. Le service RMS (Rights Management Service) est un service Microsoft qui empêche l'accès non autorisé aux documents. Si vous avez un serveur RMS configuré pour protéger vos documents, ces fichiers figureront alors sous Protection RMS.
Nom de la détection	Permet de rechercher un élément détecté en fonction de son nom.
Numéro de ticket	Permet d'effectuer la recherche d'un élément d'après le numéro de ticket, lequel désigne un identificateur alphanumérique unique affecté à une détection spécifique. Il permet d'identifier la détection associée.
Analysé par	Permet d'effectuer une recherche par nom d'analyse. Par exemple, A la demande ou A l'accès (API WSS VS) .
Nom de la stratégie	Permet de rechercher un élément en fonction d'un nom de stratégie tel qu'une Stratégie principale ou une sous-stratégie ayant détecté l'élément.
Raison	Permet de rechercher un élément en fonction de la raison de sa détection. Les raisons sont les suivantes : <ul style="list-style-type: none"> • Antivirus • Conformité et DLP • Filtre de fichiers • Crypté ou corrompu • Programme potentiellement indésirable • Packer • Crypté • Signé • Corrompu • Déni de service • Contenu protégé • Protégé par mot de passe • Sur échec d'analyse

Options de recherche supplémentaires

Le tableau ci-dessous présente des informations sur les options de recherche supplémentaires mises à votre disposition pour affiner les résultats de la recherche relatifs aux éléments détectés.

Tableau 4-2 Définition des options



Option	Définition
Toutes les dates	Permet de rechercher des éléments parmi toutes les dates.  Les résultats de la recherche sont présentés en fonction de leur date de stockage dans la base de données des éléments mis en quarantaine.
Plage de dates	Permet de rechercher un élément dans une plage de dates définie conformément à vos exigences. Cette option vous permet de spécifier la date, le mois, l'année et l'heure de comparaison par rapport aux paramètres De et A . Vous pouvez également spécifier une plage de dates à l'aide de l'icône de calendrier.  La plage de dates est définie en fonction de l'heure système locale.

Tableau 4-2 Définition des options (suite)

Option	Définition
Rechercher	Permet d'afficher la liste des éléments mis en quarantaine qui correspondent aux critères de recherche figurant dans la section Afficher les résultats .
Effacer le filtre	Permet de rétablir les paramètres de recherche par défaut.

Recherche parmi les éléments détectés


Les filtres de recherche vous permettent de trouver les éléments mis en quarantaine qui vous intéressent et d'entreprendre les actions correspondantes.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Eléments détectés**.
- 2 Dans le volet gauche, cliquez sur la catégorie de détection souhaitée telle que **Virus**, **Programmes potentiellement non désirables**, **Messages/types de fichiers interdits**, **Conformité et DLP**, **Contenu indésirable** ou **Tous les éléments**.
- 3 Dans le volet **Rechercher**, sélectionnez les filtres de recherche souhaités dans les listes déroulantes (le cas échéant). Les options de recherche disponibles sont les suivantes :

Tableau 4-3 Options de recherche

Fonctionnalité de recherche	Description
Filtre de recherche principal	<p>Choisissez d'affiner vos critères de recherche en fonction d'un filtre donné tel que Nom de la stratégie, Action entreprise, Expéditeur etc.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Pour plus d'informations sur tous les filtres de recherche principaux, consultez la section <i>Principaux filtres de recherche disponibles</i>.</p> </div>
Plage de dates	<p>Choisissez d'affiner votre recherche en utilisant toutes les dates ou une période définie.</p> <ul style="list-style-type: none"> • Toutes les dates • Plage de dates

- 4 Cliquez sur **Rechercher**.

Cette tâche vous a permis de rechercher les seuls éléments détectés correspondant à vos critères de recherche, éléments figurant désormais dans la section **Afficher les résultats**.






Pour limiter le nombre d'éléments mis en quarantaine devant s'afficher dans le volet **Afficher les résultats**, modifiez la valeur de l'option **Taille maximale de la requête (enregistrements)** via **Paramètres et diagnostics** | **Eléments détectés** | **Base de données locale**.

Actions pouvant être entreprises concernant les éléments mis en quarantaine



Affichez les résultats de la recherche en fonction des paramètres que vous avez définis et entreprenez les actions nécessaires concernant les éléments mis en quarantaine.

Vous pouvez alors exécuter ces actions sur les éléments mis en quarantaine.

Tableau 4-4 Types d'action

Action	Définition
Télécharger	<p>Permet de télécharger un élément mis en quarantaine à des fins de recherche ou d'analyse. Sélectionnez un enregistrement applicable dans le volet Afficher les résultats, puis cliquez sur Télécharger.</p> <p> Vous ne pouvez pas Télécharger plusieurs enregistrements simultanément.</p>
Exporter vers un fichier .CSV	<p>Permet d'exporter et d'enregistrer des informations concernant tous les éléments mis en quarantaine renvoyés par la recherche au format .CSV. Si la base de données comprend des milliers d'éléments mis en quarantaine, vous pouvez, plutôt que de parcourir plusieurs pages, utiliser cette option pour télécharger ces enregistrements dans un fichier au format CSV et générer par la suite des rapports personnalisés dans Microsoft Excel.</p> <p>Accédez au volet Afficher les résultats, puis cliquez sur Exporter vers un fichier .CSV pour Ouvrir les résultats de la recherche ou les Enregistrer dans le dossier ou à l'emplacement voulu.</p> <p> <ul style="list-style-type: none"> • Si un champ donné est introuvable dans le résultat de la recherche du fichier CSV, veillez à activer le champ requis sous l'option Colonnes à afficher. • Pour ouvrir le fichier CSV avec des paramètres régionaux différents, utilisez l'option Importer des données de Microsoft Excel. </p>
Colonnes à afficher	Permet de sélectionner d'autres en-têtes de colonne à répertorier dans le volet Afficher les résultats . Cette option présente une liste de tous les filtres disponibles dans le volet Rechercher ainsi que des options supplémentaires.
Sélectionner tout	Permet de sélectionner tous les éléments mis en quarantaine apparaissant dans cette page de la section Afficher les résultats . Par exemple, si 100 éléments sont en quarantaine et que vous définissez un affichage de 10 éléments par page , alors seulement 10 éléments figurant dans la section Afficher les résultats sont sélectionnés.
Ne rien sélectionner	Permet de désélectionner tous les éléments en quarantaine figurant dans la section Afficher les résultats .
Supprimer	<p>Permet de supprimer les éléments en quarantaine que vous avez sélectionnés dans cette page de la section Afficher les résultats.</p> <p> Appuyez sur la touche Ctrl et maintenez-la enfoncée pour sélectionner plusieurs éléments à la fois.</p>
Supprimer tout	Permet de supprimer de la base de données tous les éléments mis en quarantaine pour la catégorie sélectionnée.
Éléments affichés par page	<p>Permet de spécifier le nombre maximal d'éléments mis en quarantaine à afficher par page. Les options sont les suivantes :</p> <ul style="list-style-type: none"> • 10 • 20 • 50 • 100

Chaque élément figurant dans le volet **Afficher les résultats** possède une image, dont la signification est la suivante :

Icône	Description
	Élément mis en quarantaine et pouvant être téléchargé.
	Élément consigné et impossible à télécharger.

Éléments détectés

Actions pouvant être entreprises concernant les éléments mis en quarantaine

5

Gestionnaire de stratégies

Vous avez la possibilité de configurer ou de gérer différentes stratégies et les actions correspondantes dans le produit.

Une stratégie se définit généralement comme un principe ou une règle visant à orienter les décisions et à obtenir des résultats logiques. Les stratégies sont adoptées au sein d'une organisation en vue d'aider à la prise de décision des objectifs.

Dans McAfee Security for Microsoft SharePoint, une stratégie spécifie les paramètres utilisés et les actions à prendre suite au déclenchement d'une détection. Vous pouvez créer plusieurs stratégies et définir les paramètres et actions particuliers correspondants. Par exemple, vous pouvez définir plusieurs sous-stratégies pour l'option de menu **A l'accès** et configurer un paramètre et une action propres à chaque stratégie.



Faites appel à l'option de menu **Ressource partagée** située sous **Gestionnaire de stratégies** pour modifier ou créer des règles à associer aux paramètres d'analyseur, de filtre et d'alerte depuis un emplacement commun. L'option **Ressource partagée** permet de gagner du temps lors de la création et de l'application de stratégies.

Sommaire

- ▶ *Options de menu du gestionnaire de stratégies*
- ▶ *Catégories de stratégies de gestion des menaces*
- ▶ *Types d'affichage du gestionnaire de stratégies*
- ▶ *Stratégie principale et sous-stratégie*
- ▶ *Analyseurs et filtres de base*
- ▶ *Affichage de la liste des analyseurs et filtres associés à une stratégie*
- ▶ *Ajouter un analyseur ou un filtre*
- ▶ *Créer des règles de stratégie*
- ▶ *Actions pouvant être entreprises concernant les détections*
- ▶ *Ressource partagée*
- ▶ *Gestion des paramètres d'analyseur de base d'une stratégie*
- ▶ *Gestion des paramètres de filtre associés à une stratégie*

Options de menu du gestionnaire de stratégies

Affichez les options de menu disponibles sous **Gestionnaire de stratégies**.

A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies**. Les options de menu suivantes s'affichent dans le volet de navigation.

Option	Description
A l'accès	Contient des stratégies relatives aux fichiers et documents chaque fois que ceux-ci font l'objet d'un chargement ou téléchargement, afin de contrôler la présence de virus ou d'autres menaces.
A la demande	Inclut les stratégies activées à des intervalles définis ou à la demande, destinées à rechercher un virus ou toute autre menace.
Ressource partagée	Emplacement commun permettant de modifier les paramètres relatifs aux analyseurs, aux filtres, aux alertes, aux dictionnaires de conformité et DLP et aux plages horaires.

Catégories de stratégies de gestion des menaces

Affichez les catégories de stratégies disponibles et mettez en œuvre une stratégie par défaut existante (désignée sous le nom de *stratégie principale*) à votre organisation entière.

Le logiciel permet de réduire les menaces électroniques grâce à un ensemble particulier de règles et de paramètres appelé « stratégies » que vous pouvez créer selon les besoins de votre organisation.

Lorsque vous installez pour la première fois le logiciel sur votre serveur, une **stratégie principale** par défaut est disponible pour ces options de menu :

- A l'accès
- A la demande

Vous avez la possibilité de personnaliser les stratégies sous chacune de ces catégories afin de gérer avec précision des menaces spécifiques susceptibles d'avoir des répercussions sur votre serveur SharePoint.

Types d'affichage du gestionnaire de stratégies

Affichez et triez les sous-stratégies en fonction de l'héritage ou de la priorité.

Les types d'affichage du **Gestionnaire de stratégies** sont les suivants :

- Affichage d'héritage
- Affichage avancé

Affichage d'héritage

Affiche l'ordre de priorité et le statut de la stratégie principale et de toutes les sous-stratégies. Le logiciel prend une action concernant un élément selon les paramètres configurés pour la sous-stratégie dotée de la priorité la plus élevée. Lorsque les règles d'une sous-stratégie ne sont pas satisfaites, la sous-stratégie disposant de la priorité suivante est prise en compte. Les paramètres configurés dans la stratégie principale sont appliqués lorsque les règles d'aucune sous-stratégie ne sont satisfaites.

Lorsque vous sélectionnez **Affichage d'héritage**, les sous-stratégies sont visibles en fonction de l'héritage de la stratégie.

Ce type d'affichage vous permet d'effectuer les tâches suivantes :

- Affichage de la stratégie et de son niveau de priorité
- Affichage de la sous-stratégie héritée et de sa stratégie parente

- Activation ou désactivation des sous-stratégies
- Suppression des sous-stratégies

Affichage avancé

Affiche toutes les stratégies par ordre croissant, en fonction du niveau de priorité, et propose une option de modification de la priorité d'une sous-stratégie.

Ce type d'affichage vous permet d'effectuer les tâches suivantes :

- Affichage des stratégies triées par ordre de priorité
- Modification du niveau de priorité d'une stratégie



Les icônes suivantes permettent de modifier le niveau de priorité d'une stratégie :

- ▲ : augmente le niveau de priorité d'une stratégie.
- ▼ : diminue le niveau de priorité d'une stratégie.

- Activation ou désactivation des sous-stratégies
- Suppression des sous-stratégies
- Modification du nom d'une stratégie, de sa description et de la stratégie parente via un clic sur **Détails**

Stratégie principale et sous-stratégie

En général, un paramètre de stratégie situé au sein d'une structure hiérarchique est transmis du parent aux enfants, des enfants aux petits-enfants et ainsi de suite. Ce concept est appelé l'héritage. La stratégie parente par défaut est désignée par l'expression **Stratégie principale** tandis que la stratégie enfant est nommée **Sous-stratégie**.

Stratégie principale

Il s'agit de la stratégie parente par défaut, mise à disposition pour toutes les catégories de stratégies qui définissent le mode d'application de l'analyse antivirus aux éléments, le mode de filtrage des fichiers et différents autres paramètres.



Vous ne pouvez pas supprimer la **Stratégie principale**, car elle sert de référence de base pour la création de sous-stratégies.

Sous-stratégie

Une stratégie qui hérite des paramètres et actions d'une autre stratégie est appelée sous-stratégie.

Les sous-stratégies sont nécessaires dans les situations où vous auriez besoin d'exceptions à la **Stratégie principale** afin de répondre aux exigences de zones géographiques, de fonctions, de domaines ou de services particuliers de votre organisation.

L'action entreprise concernant un élément dépend des paramètres configurés pour la sous-stratégie dotée de la priorité la plus élevée. Lorsque les règles d'une sous-stratégie dotée de la priorité la plus élevée ne sont pas satisfaites, le logiciel passe à la sous-stratégie disposant de la priorité suivante. Les paramètres configurés dans la stratégie principale sont uniquement appliqués lorsque les règles d'aucune sous-stratégie ne sont satisfaites.

Si vous sélectionnez l'option **Hériter de tous les paramètres de la stratégie parente** à la page des paramètres d'analyseur ou de filtre, une stratégie (sous-stratégie) héritée met en œuvre le même paramètre que la stratégie parente. Cependant, en cas de détection, vous pouvez entreprendre une action différente. Les modifications apportées aux paramètres dans la stratégie parente ou la **Stratégie principale** sont reflétées dans ces sous-stratégies.



La restauration du paramètre par défaut du logiciel entraîne la suppression des sous-stratégies existantes. Assurez-vous de sauvegarder les stratégies et les paramètres à l'aide de l'option **Exporter**, disponible sous l'onglet **Paramètres et diagnostics | Importer et exporter la configuration | Configuration**, avant de restaurer les paramètres d'usine du produit.

Création de sous-stratégies

Créez des stratégies supplémentaires basées sur la **Stratégie principale** ou sur une stratégie parente en fonction des besoins propres à une section donnée de votre organisation. Vous pouvez créer des sous-stratégies destinées à couvrir des situations exceptionnelles, non prises en compte par la **Stratégie principale**.

Cette méthode s'avère pratique pour ne pas appliquer les règles de la **Stratégie principale** à certains types de fichiers de votre organisation. Vous pouvez ainsi créer des exceptions et permettre au logiciel d'effectuer une analyse particulière.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégie** et sélectionnez une rubrique de menu pour laquelle vous voulez créer une sous-stratégie.
- 2 Cliquez sur **Créer une sous-stratégie**.
La page **Créer une sous-stratégie** s'affiche.
- 3 Sous **Configuration initiale | Identification | Nom de la sous-stratégie**, spécifiez un nom permettant d'identifier la stratégie et son rôle.
- 4 Tapez une **Description** de la stratégie (facultatif).
- 5 Sélectionnez la **Stratégie parente** dont la sous-stratégie hérite les paramètres.
- 6 Cliquez sur **Suivant**.
- 7 Sous **Règles de déclenchement | Spécifier des règles de stratégie**, cliquez sur **Nouvelle règle** pour créer une nouvelle règle.
La page **Spécifier une règle de stratégie** s'affiche.
- 8 Sous **Spécifier une règle de stratégie**, vous pouvez sélectionner les options suivantes :
 - **<sélectionnez un modèle de règle>** : permet de spécifier une règle de stratégie en fonction du nom du fichier. Vous pouvez créer des règles basées sur les options suivantes :
 - **Le nom du fichier est le nom du fichier**
 - **Le nom du fichier n'est pas le nom du fichier**
 - **Copier les règles d'une autre stratégie** : permet de copier les règles à partir d'une autre stratégie.

- 9 Spécifiez les conditions dans lesquelles la stratégie doit se déclencher pour l'utilisateur. Vous pouvez sélectionner :
- **Au moins une des règles s'applique** : permet de spécifier si l'une des règles s'applique à la stratégie.
 - **Toute les règles s'appliquent** : permet de spécifier si toutes les règles créées s'appliquent à la stratégie.
 - **Aucune des règles ne s'applique** : permet de spécifier si aucune des règles créées ne s'applique à la stratégie.
- 10 Cliquez sur **Ajouter**.



Pour supprimer une règle, sélectionnez la règle et cliquez sur **Supprimer**.

- 11 Cliquez sur **Suivant**.
- 12 Sous **Analyseurs et filtres**, vous pouvez sélectionner :
- **Hériter de tous les paramètres de la stratégie parente** : permet d'hériter de toutes les propriétés de la stratégie parente.
 - **Initialiser les paramètres sélectionnés avec les valeurs copiées d'une autre stratégie** : permet de sélectionner des analyseurs et des filtres précis parmi les stratégies disponibles. Vous pouvez sélectionner et désélectionner n'importe quel analyseur ou filtre.
- 13 Cliquez sur **Terminer**.

Vous avez à présent terminé la création d'une sous-stratégie.

Analyseurs et filtres de base

Déterminent les types d'analyseur et de filtre qui peuvent être appliqués lors de la création de stratégies.

Analyseurs de base

Affichez et configurez les paramètres relatifs à ces analyseurs via **Gestionnaire de stratégies** | **A l'accès**.

Analyseur	Définition
Analyseur antivirus	Permet de configurer les paramètres destinés à détecter les menaces de type virus, chevaux de Troie, vers, programmes de compression, logiciels espions (spyware), logiciels publicitaires (adware), etc.
Analyseur de conformité et DLP	Permet de créer ou de configurer des Règles de conformité et DLP conformes aux stratégies de confidentialité et de conformité de votre organisation, avec l'ajout de 60 nouveaux Dictionnaires de conformité et DLP .
Filtrage des fichiers	Permet de créer de nouvelles règles de filtrage de fichiers répondant aux besoins de votre organisation. Configurez ces paramètres afin de détecter les fichiers en fonction de leur nom, de leur catégorie ou de leur taille.

Filtres

Spécifiez les actions à prendre en cas de détection, en fonction des besoins de votre organisation.

Filtre	Définition
Contenu corrompu	Permet de configurer les paramètres destinés à définir l'action à prendre concernant les éléments au contenu corrompu.
Contenu protégé	Permet de configurer les paramètres destinés à définir l'action à prendre concernant les éléments au contenu protégé.
Contenu crypté	Permet de configurer les paramètres destinés à définir l'action à prendre concernant les éléments au contenu chiffré.
Contenu signé	Permet de configurer les paramètres destinés à définir l'action à prendre concernant les éléments au contenu signé.
Fichiers protégés par mot de passe	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les éléments contenant des fichiers protégés par mot de passe.
Contrôle de l'analyseur	Permet de créer ou de configurer les paramètres de l'analyseur de base destinés à définir l'action à prendre concernant les éléments en fonction de leur niveau d'imbrication, de la taille du fichier décompressé et de la durée d'analyse.

Affichage de la liste des analyseurs et filtres associés à une stratégie

Affichez le statut des analyseurs et filtres disponibles pour la catégorie de stratégies sélectionnée.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies**, puis sur l'élément de menu désignant la catégorie de stratégies voulue.

La page de stratégie relative à l'élément de menu sélectionné s'affiche.

- 2 Cliquez sur **Stratégie principale** ou sur la sous-stratégie requise.

La page de stratégies correspondante s'affiche.

- 3 La page de stratégies propose les onglets suivants :

- **Afficher la liste de tous les analyseurs** : permet d'afficher l'analyseur ou le filtre activé pour la stratégie.
- **Afficher les paramètres** : permet d'afficher les paramètres de l'analyseur ou du filtre, et les actions spécifiées.
- **Spécifier des règles** : permet de spécifier les règles de stratégie qui s'appliquent à des types précis d'éléments ou de fichiers.





Vous pouvez spécifier des règles de stratégie uniquement à des sous-stratégies.

- 4 Sous l'onglet **Afficher la liste de tous les analyseurs**, vous pouvez utiliser les options suivantes :

Tableau 5-1 Configuration de la stratégie

Option	Définition
Stratégie	Permet de sélectionner la stratégie à configurer.
Ajouter un analyseur/filtre	Permet de configurer la stratégie de sorte qu'elle ne s'applique qu'à des moments particuliers. Par exemple, vous pouvez créer un nouveau paramètre antivirus comprenant différentes règles qui s'applique uniquement le week-end.

Tableau 5-1 Configuration de la stratégie (suite)

Option	Définition
Analyseurs noyaux	Permet de configurer la stratégie de chacun des analyseurs suivants : <ul style="list-style-type: none"> • Analyseur antivirus • Analyseur de conformité et DLP • Filtrage des fichiers
Filtres	Permet de configurer la stratégie de chacun des filtres suivants : <ul style="list-style-type: none"> • Contenu corrompu • Contenu protégé • Contenu crypté • Contenu signé • Fichiers protégés par mot de passe • Contrôle de l'analyseur
Hérite	Permet de spécifier si les analyseurs et filtres de base sont hérités de la stratégie principale. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <ul style="list-style-type: none"> •  indique si l'analyseur ou le filtre est hérité. • Cela n'est pas valable pour la stratégie principale. </div>

Ajouter un analyseur ou un filtre

Ajoutez un analyseur ou un filtre pour définir des paramètres propres à des scénarios exceptionnels dans votre organisation.

Il est pratique d'ajouter un analyseur ou un filtre pour disposer d'un analyseur ou d'un filtre supplémentaire :

- comprenant des options et des règles différentes ;
- à activer uniquement pendant une plage horaire précise.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez une catégorie de stratégies.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie.
- 3 Sous l'onglet **Afficher la liste de tous les analyseurs**, cliquez sur **Ajouter un analyseur/filtre**.
- 4 Dans la liste déroulante **Spécifier la catégorie**, sélectionnez l'analyseur ou le filtre requis.

- 5 Dans la section **Quand utiliser cette instance**, sélectionnez un créneau horaire existant ou créez-en un nouveau.
- **Sélectionner un créneau horaire existant**— Sélectionnez cette option pour choisir l'un de ces créneaux horaires existants.
 - **Créer un nouveau créneau horaire** — Cette option permet de créer un nouveau créneau horaire. Spécifiez les options suivantes :

Option	Définition
Nom de créneau horaire significatif	Attribuez un nom au créneau horaire, par exemple Week-end ou Semaine.
Sélectionner le jour et l'heure	Sélectionnez le jour de la semaine voulu.
Toute la journée	Sélectionnez cette option pour spécifier toute la journée.
Heures sélectionnées	Sélectionnez cette option pour spécifier l'heure de début et l'heure de fin.

- 6 Cliquez sur **Enregistrer**.
- 7 Cliquez sur **Appliquer**.



Modifiez les options et les règles en fonction des besoins de votre organisation.

Créer des règles de stratégie

Elaborez de nouvelles règles et spécifiez les conditions à appliquer à une stratégie.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez une catégorie de stratégies.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie.
- 3 Cliquez sur l'onglet **Spécifier des règles**.
- 4 Cliquez sur **Nouvelle règle**.
- 5 Sous **Spécifier une règle de stratégie**, vous pouvez sélectionner les options suivantes :
 - **<sélectionnez un modèle de règle>** : permet de spécifier une règle de stratégie en fonction du nom du fichier. Vous pouvez créer des règles basées sur les options suivantes :
 - **Le nom du fichier est le nom du fichier**
 - **Le nom du fichier n'est pas le nom du fichier**
 - **Copier les règles d'une autre stratégie** : permet de copier les règles à partir d'une autre stratégie.
- 6 Cliquez sur **Ajouter**.
- 7 Pour supprimer une règle, sélectionnez la règle et cliquez sur **Supprimer**.

- 8 Précisez les conditions dans lesquelles la stratégie doit se déclencher. Vous pouvez sélectionner :
- **Au moins une des règles s'applique** — Permet de spécifier si l'une des règles s'applique à la stratégie.
 - **Toute les règles s'appliquent** — Permet de spécifier si toutes les règles créées s'appliquent à la stratégie.
 - **Aucune des règles ne s'applique** — Permet de spécifier si aucune des règles créées ne s'applique à la stratégie.
- 9 Cliquez sur **Appliquer** pour enregistrer la règle.

Actions pouvant être entreprises concernant les détections

Vous avez la possibilité, pour tous les paramètres d'analyseur et de filtre d'une stratégie, de spécifier une action principale et une action secondaire à entreprendre concernant une détection. Vous pouvez spécifier la manière dont doit être traité un élément, quand il déclenche une détection.

Lorsqu'une règle de stratégie est déclenchée d'après les paramètres d'analyseur ou de filtre, le logiciel traite la détection en fonction des actions principale et secondaire configurées.

Lorsque vous configurez des actions, vous devez sélectionner au moins une action principale. Vous pouvez également sélectionner plusieurs actions secondaires. Par exemple, si l'action principale empêche le chargement/téléchargement d'un élément ayant déclenché une détection, l'action secondaire peut consister à consigner la détection dans un journal et à la mettre en quarantaine.

Les actions principales disponibles varient en fonction du type de catégorie de stratégies et des paramètres d'analyseur ou de filtre configurés.



Cliquez sur **Réinitialiser** afin de restaurer les paramètres par défaut des actions pour la catégorie de stratégies et l'analyseur.

Tableau 5-2 Actions principales

Action	Définition
Tenter de nettoyer tout virus ou cheval de Troie détecté	Permet de nettoyer un élément contenant un virus ou un cheval de Troie détecté par l'Analyseur antivirus.
Remplacer l'élément par une alerte	Permet de remplacer par une alerte l'élément ayant déclenché la détection.
Supprimer l'élément incorporé	Permet de remplacer la pièce jointe ayant déclenché la détection dans un document.
Empêcher le chargement/téléchargement de l'élément	Permet d'empêcher le chargement ou le téléchargement de l'élément ayant déclenché la détection.
Autoriser	Permet d'autoriser l'élément à poursuivre jusqu'à la phase suivante.

Tableau 5-3 Actions secondaires

Action	Définition
Consigner dans les éléments détectés	Permet d'enregistrer la détection dans un journal.
Quarantaine	Permet de conserver dans la base de données de quarantaine une copie de l'élément ayant déclenché la détection. Pour afficher tous les éléments mis en quarantaine, accédez à Eléments détectés Tous les éléments ou choisissez une catégorie de détections précise.

Ressource partagée

Emplacement commun permettant de modifier les paramètres relatifs aux analyseurs, aux filtres, aux alertes, aux dictionnaires de conformité et DLP et aux plages horaires. Lors de la configuration de stratégies, vous pouvez choisir d'appliquer la même ressource (paramètres d'analyseur et de filtre) à plusieurs stratégies. Dans ce type de scénario, utilisez l'option **Ressource partagée**.

A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**. Vous pouvez utiliser les onglets suivants :

- **Analyseurs et alertes** : permet de modifier ou de créer des paramètres d'analyseur et de filtre.
- **Dictionnaires de conformité et DLP** : permet de modifier ou de créer des règles sous **Règles de conformité et DLP** et **Règles de filtrage des fichiers**.
- **Créneaux horaires** : permet de modifier ou de créer des plages horaires de type jours de la semaine ou week-ends.



Les modifications apportées à ces paramètres sont automatiquement répercutées sur toutes les stratégies ayant recours à ces configurations.

Configuration des paramètres de l'analyseur

Créez ou modifiez des paramètres d'analyseur en fonction des exigences de votre organisation.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.
La page **Ressources partagées** s'affiche.
- 2 Cliquez sur l'onglet **Analyseurs et alertes**.
- 3 Dans la liste déroulante **Catégorie**, sous la section **Analyseurs**, sélectionnez l'analyseur à configurer. Le type d'analyseur s'affiche avec le nom des paramètres, les stratégies qui l'utilisent et l'action à configurer. Vous pouvez utiliser les options suivantes :

Tableau 5-4 Définition des options

Option	Définition
Catégorie	Permet de sélectionner l'analyseur requis à configurer.
Créer une nouvelle catégorie	Permet de créer de nouveaux paramètres pour un analyseur en fonction de vos exigences. Cette option s'avère nécessaire dans les situations exigeant des exceptions pour certains paramètres d'analyseur et doit être appliquée dans une stratégie.
Modifier	Permet de modifier les paramètres de l'analyseur sélectionné.
Supprimer	Permet de supprimer les paramètres de l'analyseur.

Vous ne pouvez pas supprimer un analyseur, s'il s'agit d'un analyseur par défaut et s'il est utilisé par une stratégie. Pour savoir par combien de stratégies ce paramètre d'analyseur est utilisé, consultez la colonne **Utilisé par**.

- 4 Dès lors que vous avez configuré les paramètres de l'analyseur, cliquez sur **Enregistrer**, puis sur **Appliquer**.

Configuration des paramètres d'alerte

Créez ou modifiez des paramètres d'alerte pour l'analyseur sélectionné en fonction des exigences de votre organisation.



Les paramètres d'alerte s'appliquent uniquement aux stratégies à la demande.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.
La page **Ressources partagées** s'affiche.
- 2 Cliquez sur l'onglet **Analyseurs et alertes**.
- 3 Dans la liste déroulante **Catégorie**, sous la section **Alertes**, sélectionnez l'alerte à configurer pour un analyseur. Le type d'analyseur s'affiche avec le nom des paramètres, les stratégies qui l'utilisent et l'action à configurer. Vous pouvez utiliser les options suivantes :

Tableau 5-5 Définition des options

Option	Définition
Catégorie	Permet de sélectionner l'analyseur requis à configurer.
Créer une nouvelle catégorie	Permet de créer de nouveaux paramètres pour un analyseur en fonction de vos exigences. Cette option s'avère nécessaire dans les situations exigeant des exceptions pour certains paramètres d'analyseur et doit être appliquée dans une stratégie.
Afficher	Permet de visualiser les paramètres d'alerte par défaut d'un analyseur.
Modifier	Permet de modifier les paramètres de l'analyseur sélectionné.
Supprimer	Permet de supprimer les paramètres de l'analyseur.

Vous ne pouvez pas supprimer une alerte s'il s'agit d'une alerte d'analyseur par défaut et si elle est utilisée par une stratégie. Pour savoir par combien de stratégies ce paramètre d'alerte est utilisé, consultez la colonne **Utilisé par**.

- 4 Dès lors que vous avez configuré les paramètres de l'analyseur, cliquez sur **Enregistrer**, puis sur **Appliquer**.

Vous avez à présent terminé la configuration des paramètres d'une alerte en fonction des exigences de votre organisation.

Création d'une nouvelle alerte

Créez un nouveau message d'alerte pour les actions entreprises par un analyseur ou un filtre.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.
La page **Ressources partagées** s'affiche.
- 2 Cliquez sur l'onglet **Analyseurs et alertes**.
- 3 Dans la liste déroulante **Catégorie**, sous la section **Alertes**, sélectionnez l'alerte à configurer pour un analyseur.

- 4 Cliquez sur **Créer une nouvelle catégorie**.

La page **Editeur d'alerte** s'affiche.

- 5 Tapez un **Nom d'alerte** explicite.

- 6 Sélectionnez les valeurs requises dans les listes déroulantes **Style**, **Police** et **Taille**.



Ces options sont uniquement disponibles lorsque l'option **Contenu HTML (WYSIWYG)** est sélectionnée dans le menu déroulant **Afficher**.

- 7 Sélectionnez les valeurs que vous voulez inclure dans votre message d'alerte à partir de la liste déroulante **Jetons**.
 - **DÉTECTIONS** — Liste des détections dans l'élément.
 - **ATTACHMENTNAME** — Nom de l'élément en cours d'analyse.
 - **ACTIONNAME** — Actions prises concernant l'élément.
 - **AVDATVERSION** — Version des fichiers DAT utilisés par le moteur antivirus.
 - **AVENGINEVERSION** — Version du moteur antivirus.
 - **TICKETNUMBER** — Entrée alphanumérique de 16 chiffres qui est générée automatiquement par le logiciel pour chaque détection.

8 Personnalisez l'alerte en utilisant l'un des outils suivants :



Tableau 5-6 Options de la barre d'outils

Options	Description
Gras	Permet de mettre en gras le texte sélectionné.
Italique	Permet de mettre en italique le texte sélectionné.
Souligné	Permet de souligner le texte sélectionné.
Aligner à gauche	Permet d'aligner à gauche le paragraphe sélectionné.
Centrer	Permet de centrer le paragraphe sélectionné.
Aligner à droite	Permet d'aligner à droite le paragraphe sélectionné.
Justifier	Permet d'ajuster le paragraphe sélectionné de sorte que les lignes du paragraphe remplissent une largeur donnée, avec les bords gauche et droit alignés.
Liste classée	Permet d'ordonner le texte sélectionné dans une liste numérotée.
Liste non classée	Permet d'ordonner le texte sélectionné dans une liste à puces.
Retrait négatif	Permet de déplacer le texte sélectionné à une distance définie vers la droite.
Retrait	Permet de déplacer le texte sélectionné à une distance définie vers la gauche.
Couleur du texte	Permet de modifier la couleur du texte sélectionné.
Couleur d'arrière-plan	Permet de modifier la couleur d'arrière-plan du texte sélectionné.
Règle horizontale	pour insérer une ligne horizontale.
Insérer un lien	Permet d'insérer un lien hypertexte à l'endroit où est actuellement positionné le curseur. Dans URL , tapez l' URL . Dans Texte , tapez le nom du lien hypertexte tel que vous voulez qu'il apparaisse dans le message d'alerte. Si vous voulez que le lien ouvre une nouvelle fenêtre, sélectionnez Ouvrir le lien dans une nouvelle fenêtre , puis cliquez sur Insérer un lien .
Insérer une image	Permet d'insérer une image à l'endroit où est actuellement positionné le curseur. Dans URL de l'image , tapez l'emplacement de l'image. Dans Texte de remplacement , entrez le texte qui apparaît à la place de l'image lorsque celle-ci est supprimée ou que le message d'alerte s'affiche dans un navigateur textuel. Si vous voulez donner un titre à l'image, tapez-le dans Utiliser ce texte comme titre de l'image . Cliquez sur Insérer une image .
Insérer un tableau	Permet d'insérer un tableau à l'endroit où est actuellement positionné le curseur. Insérez des valeurs dans Lignes , Colonnes , Largeur du tableau , Epaisseur de la bordure , Remplissage des cellules et Espacement des cellules pour configurer le tableau, puis cliquez sur Insérer un tableau .

- 9 Dans le menu déroulant **Afficher**, spécifiez la manière dont le message d'alerte doit s'afficher dans l'interface utilisateur. Vous pouvez sélectionner :
 - **Contenu HTML (WYSIWYG)** — Permet de masquer le code HTML sous-jacent et d'afficher uniquement le contenu du message d'alerte.
 - **Contenu HTML (source)** — Permet d'afficher le message d'alerte avec le code HTML tel qu'il apparaît avant compilation.
 - **Contenu en texte brut** — Permet d'afficher le contenu sous la forme de texte brut.
- 10 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.



Cliquez sur **Réinitialiser** pour annuler toutes les modifications effectuées depuis le dernier enregistrement du message d'alerte.

Configuration des règles de conformité et DLP




Créez ou modifiez des règles et dictionnaires de conformité et de prévention des fuites de données (DLP) en fonction des exigences de votre organisation.


Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.
La page **Ressources partagées** s'affiche.
- 2 Cliquez sur l'onglet **Dictionnaires de conformité et DLP**.
- 3 Dans la liste déroulante **Catégorie**, sous la section **Règles de conformité et DLP**, sélectionnez la catégorie à afficher ou à configurer. Le groupe de règles s'affiche avec le nom, les stratégies qui l'utilisent et l'action à configurer. Vous pouvez utiliser les options suivantes :

Tableau 5-7 Définition des options

Option	Définition
Catégorie	<p>Permet de sélectionner l'analyseur requis à configurer. Cette distribution comprend 60 dictionnaires de conformité et DLP supplémentaires, garantissant que le contenu est conforme aux stratégies de confidentialité et de conformité de votre organisation.</p> <p>Caractéristiques des dictionnaires de conformité prédéfinis :</p> <ul style="list-style-type: none"> • Ajout de 60 nouveaux dictionnaires de conformité et DLP • Prise en charge de dictionnaires de conformité propres au secteur : HIPAA, PCI, code source (Java, C++, etc.) <p>Ces dictionnaires sont classés par catégories :</p> <ul style="list-style-type: none"> • Dictionnaires basés sur le score : une règle est déclenchée lorsqu'un document dépasse le seuil de score et le nombre maximal de termes, ce qui se traduit par une réduction des faux positifs. • Dictionnaires non basés sur le score : une règle est déclenchée lorsqu'un mot ou une expression spécifique est identifié(e) dans le document. <p> Pour des informations sur les dictionnaires basés sur le score et les dictionnaires non basés sur le score, consultez <i>Configuration des paramètres d'analyseur de conformité et DLP</i>.</p>
Nouvelle catégorie	<p>Permet de créer un nouveau dictionnaire de Règles de conformité et DLP.</p> <p> Toute nouvelle catégorie ou condition créée ne dépend pas du score.</p>
Créer une nouvelle catégorie	<p>Permet de créer un nouveau groupe de règles pour la catégorie sélectionnée en fonction de vos exigences. Cette option s'avère nécessaire dans les situations exigeant des règles précises pour déclencher une détection et doit être appliquée dans une stratégie.</p>
Modifier	<p>Permet de modifier les paramètres de la règle Conformité et DLP sélectionnée.</p>
Supprimer	<p>Permet de supprimer la règle Conformité et DLP.</p> <p> Vous ne pouvez pas supprimer une règle Conformité et DLP dans les cas suivants :</p> <ul style="list-style-type: none"> • Elle est activée. Désélectionnez la règle, cliquez sur Appliquer pour appliquer les paramètres, puis choisissez Supprimer. • Il est utilisé par une stratégie. Pour savoir par combien de stratégies ce paramètre d'analyseur est utilisé, consultez la colonne Utilisé par.

 Par exemple, sélectionnez **Credit Card Number** (Numéro de carte de crédit) ou tout autre dictionnaire répondant à vos besoins dans la liste déroulante **Catégorie**, puis repérez l'option **Groupe de règles améliorée** à présent disponible.

- 4 Pour créer un groupe de règles, cliquez sur **Créer une nouvelle catégorie** en regard de l'option **Règles de conformité et DLP** correspondant à la catégorie sélectionnée.

La page **Nouvelle règle d'analyseur de conformité et DLP** s'affiche pour la catégorie sélectionnée.

- 5 Tapez le **Nom de la règle** et sa **Description**.
- 6 Sélectionnez **Ajouter cette règle au groupe de règles de cette catégorie** pour ajouter la nouvelle règle au groupe de règles pour la catégorie sélectionnée.

7 Sous **Terme ou phrase**, spécifiez les mots ou les expressions à rechercher, à la section **La règle sera déclenchée lors de la détection du terme ou de la phrase suivante**. Sélectionnez ensuite l'une des options suivantes :

- **Expression régulière** : si cette option est activée, la règle est déclenchée pour le texte spécifié correspondant à une expression régulière (regex). Il s'agit d'une méthode précise et concise permettant de faire correspondre des chaînes de texte, comme des termes, des caractères ou des modèles de caractères.

Exemple : la séquence de caractères « rue » figurant à la suite dans n'importe quel contexte, comme grue, cruel ou recrue.



L'expression régulière (regex) est désactivée pour certaines expressions. Consultez <http://www.regular-expressions.info/reference.html> ou <http://www.zytrax.com/tech/web/regex.htm> pour plus de détails.

- **Utiliser des caractères génériques** : si cette option est activée, la règle se déclenche pour le terme ou l'expression spécifié(e) qui contient un ou plusieurs caractères génériques. (En général, les caractères génériques servent à remplacer un ou plusieurs caractères d'un mot inconnu ou que ne souhaitez pas saisir en entier.)
- **Débuter par** — Si activée, la règle est déclenchée pour le texte spécifié qui forme le début du mot ou de l'expression.
- **Se termine par** — Si cette option est activée, la règle se déclenche pour le texte spécifié qui constitue la dernière partie du mot ou de l'expression.
- **Sensible à la casse** — Si cette option est activée, la règle se déclenche si la casse du texte spécifié correspond au mot ou à l'expression.



Pour détecter un mot ou une expression en observant une correspondance parfaite, sélectionnez à la fois **Commence par** et **Se termine par**.

- 8 Sélectionnez l'option **Spécifier des expressions ou des termes contextuels supplémentaires**, laquelle correspond à une action secondaire une fois le terme ou l'expression principal(e) détecté(e). Spécifiez tout terme ou toute expression pouvant accompagner le mot ou l'expression principal(e) déclenchant une détection.
- 9 Sélectionnez **Déclencher si TOUTES les phrases sont présentes**, **Déclencher si N'IMPORTE LAQUELLE des phrases est présente** ou **Déclencher si AUCUNE des phrases n'est présente** dans le menu déroulant.
- 10 Sélectionnez **Au sein d'un bloc** pour indiquer le nombre de **Caractères** d'un bloc à analyser.
- 11 Cliquez sur **Ajouter un mot contextuel** pour taper des mots ou des expressions supplémentaires.
- 12 Spécifiez le mot ou l'expression dans **Spécifier des termes ou expressions**, sélectionnez l'une des conditions (mêmes options qu'à l'étape 7), puis cliquez sur **Ajouter**.
- 13 Sous **Format de fichier**, sélectionnez **Tout** afin d'activer toutes les catégories de fichiers et leurs sous-catégories. Vous pouvez sélectionner plusieurs catégories et types de fichier parmi les catégories sélectionnées qui doivent correspondre. La sélection de l'option **Tout** dans le sélecteur de sous-catégories remplace toutes les autres sélections déjà effectuées.
- 14 Si vous n'avez pas sélectionné **Tout**, cliquez sur **Effacer les sélections** pour désélectionner l'une des options de type de fichier sélectionnées.
- 15 Cliquez sur **Enregistrer** pour revenir à la page **Ressources partagées**.
- 16 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez à présent terminé la configuration des règles et dictionnaires de conformité et de prévention des fuites de données (DLP) en fonction des exigences de votre organisation.

Configuration des règles de filtrage de fichiers

Vous pouvez utiliser les règles de filtrage des fichiers pour surveiller et restreindre le déplacement de fichiers. Vous pouvez filtrer les fichiers en fonction de leur nom de fichier, type de catégorie et taille.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.

La page **Ressources partagées** s'affiche.

- 2 Cliquez sur l'onglet **Dictionnaires de conformité et DLP**.

- 3 Sous **Règles de filtrage des fichiers**, cliquez sur **Créer une nouvelle catégorie**.

La page **Règle de filtrage des fichiers** s'affiche.

- 4 Renseignez le champ **Nom de règle** en choisissant un nom unique. Il est conseillé d'attribuer un nom significatif afin de pouvoir identifier facilement les règles et leur fonction. Exemples : FichiersPlusDe5Mo ou Blocage fichiers MPP.

- 5 La page **Règle de filtrage des fichiers** vous propose les options suivantes :

Tableau 5-8 Définition des options – Filtrage par nom de fichier

Option	Définition
Activer le filtrage de noms de fichiers	Permet d'activer le filtrage de fichiers en fonction des noms de fichier.
Entreprendre une action si le nom de fichier correspond	Spécifiez le nom des fichiers déclenchant cette règle. L'utilisation de caractères génériques (* ou ?) vous permet de rechercher plusieurs noms de fichier. Par exemple, si vous voulez filtrer des fichiers Microsoft PowerPoint, tapez *.ppt.
Ajouter	Permet d'ajouter le nom de fichier spécifié sous Entreprendre une action si le nom de fichier correspond à la liste de filtrage des noms de fichier.
Modifier	Permet de modifier ou de changer une règle de filtrage de fichiers existante.
Supprimer	Permet de supprimer le nom de fichier de la liste de filtrage.


 Vous ne pouvez pas supprimer une règle de filtrage de fichiers si elle est utilisée par une stratégie. La colonne **Utilisé par** doit afficher **0 stratégies** en regard de la règle que vous souhaitez supprimer. Commencez par supprimer la règle de filtrage de fichiers au sein de la stratégie, puis cliquez sur **Supprimer**.

Tableau 5-9 Définition des options – Filtrage des catégories de fichiers

Option	Définition
Activer le filtrage de catégories de fichiers	Permet d'activer le filtrage de fichiers en fonction du type de fichier.
Entreprendre une action si la catégorie du fichier est	Spécifiez le type des fichiers affectant cette règle.


 Les types de fichier se divisent en catégories et en sous-catégories.

Tableau 5-9 Définition des options – Filtrage des catégories de fichiers (suite)

Option	Définition
Catégories de fichiers	Sélectionnez une catégorie de types de fichier. Un astérisque (*) s'affiche en regard du type de fichier pour indiquer que ce dernier sera filtré.
Sous-catégories	Sélectionnez la sous-catégorie à filtrer. Pour sélectionner plusieurs sous-catégories, utilisez la combinaison de touches Ctrl+clic ou Maj+clic . Pour sélectionner toutes les sous-catégories, cliquez sur Tout . Cliquez sur Effacer les sélections pour annuler la dernière sélection.
Etendre cette règle à des catégories de fichiers non reconnues	Permet d'appliquer cette règle à toutes les éventuelles autres catégories et sous-catégories de fichiers qui ne sont pas mentionnées dans les listes de catégories et de sous-catégories.

Tableau 5-10 Définition des options – Filtrage par taille de fichier

Option	Définition
Activer le filtrage de tailles de fichiers	Permet de filtrer les fichiers en fonction de leur taille.
Entreprendre une action si la taille du fichier est	Spécifiez une valeur dans la zone de texte adjacente, choisissez un élément dans la liste déroulante, puis sélectionnez : <ul style="list-style-type: none"> • Supérieure à : permet de spécifier que l'action doit uniquement être entreprise si la taille du fichier est supérieure à celle spécifiée. • Inférieure à : permet de spécifier que l'action doit uniquement être entreprise si la taille du fichier est inférieure à celle spécifiée.

6 Cliquez sur **Enregistrer** pour revenir à la page **Ressources partagées**.

7 Cliquez sur **Appliquer** pour créer la règle de filtrage de fichiers.

Vous avez à présent terminé la création d'une règle de filtrage de fichiers.

Configuration de plages horaires

Définissez différentes plages horaires ou configurez les plages horaires existantes de manière à les appliquer à des stratégies en fonction des exigences de votre organisation.

L'option **Créneaux horaires** vous permet de spécifier la période pendant laquelle certaines règles doivent être déclenchées. Par exemple, vous pouvez restreindre le téléchargement de fichiers volumineux pendant les heures de bureau.

Certaines situations peuvent nécessiter la mise en place de plages horaires supplémentaires, définies en fonction des utilisateurs, de leur situation géographique ou des heures de travail. Vous pouvez créer de nouvelles plages horaires en fonction des heures d'ouverture, des heures de fermeture, de la maintenance hebdomadaire et ainsi de suite.

Par défaut, le logiciel comprend les plages horaires suivantes :

- En permanence
- En semaine

- Les week-ends
- Heures travaillées



Il est impossible de supprimer ou de modifier la plage horaire par défaut **En permanence**, car la **Stratégie principale** l'utilise.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies | Ressource partagée**.
La page **Ressources partagées** s'affiche.
- 2 Cliquez sur l'onglet **Créneau horaire**.
- 3 Cliquez sur **Créer une nouvelle catégorie**.
La page **Créneau horaire** s'affiche.
- 4 Renseignez le champ **Nom du créneau horaire** en utilisant un nom unique tel **Heures d'ouverture** ou **Maintenance (hebdomadaire)** du système.
- 5 Sous **Sélectionner le jour et l'heure**, précisez les jours appropriés.
- 6 Sélectionnez **Toute la journée** ou **Heures sélectionnées**.
- 7 Si vous avez choisi **Heures sélectionnées**, spécifiez les heures de **Début** et de **Fin** dans la liste déroulante.
- 8 Cliquez sur **Enregistrer** pour revenir à la page **Ressources partagées**.
- 9 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez à présent terminé la configuration ou la création d'une plage horaire en fonction des exigences de votre organisation.

Gestion des paramètres d'analyseur de base d'une stratégie

Créez ou modifiez les options d'analyseur, puis spécifiez une action appropriée à entreprendre concernant l'élément détecté suite au déclenchement d'une stratégie.

Les analyseurs de base disponibles sont les suivants :

- **Analyseur antivirus**
- **Analyseur de conformité et DLP**
- **Filtrage des fichiers**

Procédures

- *Configuration des paramètres de l'analyseur antivirus, page 64*
Configurez dans une stratégie les paramètres disponibles sous **Analyseur antivirus** afin d'identifier, de contrer et d'éliminer les virus informatiques et autres logiciels malveillants (malware).
- *Configuration des paramètres de filtrage de fichiers, page 67*
Configurez les paramètres dans une stratégie afin de détecter les fichiers en fonction de leur nom, de leur type ou de leur taille et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres d'analyseur de conformité et DLP, page 68*
Configurez les paramètres de l'**Analyseur de conformité et DLP** dans une stratégie afin d'identifier les données des documents ou autres éléments non conformes et prendre les mesures nécessaires correspondantes.

Configuration des paramètres de l'analyseur antivirus

Configurez dans une stratégie les paramètres disponibles sous **Analyseur antivirus** afin d'identifier, de contrer et d'éliminer les virus informatiques et autres logiciels malveillants (malware).

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant l'analyseur antivirus.

La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Analyseur antivirus**.
- 4 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de l'analyseur antivirus correspondant à l'élément de sous-menu choisi.



Si vous êtes en train de configurer les paramètres d'une sous-stratégie, sélectionnez l'option **Utiliser la configuration de la stratégie parente** afin d'hériter des paramètres de la stratégie parente.


- 5 Dans la section **Options**, vous pouvez utiliser les options suivantes :

Tableau 5-11 Définition des options

Option	Définition
Protection élevée	Permet d'analyser tous les fichiers, fichiers d'archive, virus inconnus, virus de macro inconnus et programmes potentiellement indésirables, ainsi que de détecter les macros dans tous les fichiers.
Protection moyenne	Permet d'analyser tous les fichiers, fichiers d'archive, virus inconnus, virus de macro inconnus et programmes potentiellement indésirables.
Protection faible	Permet d'analyser uniquement les types de fichier par défaut, les fichiers d'archive et les programmes potentiellement indésirables.
<créer un nouveau jeu d'options>	Permet de créer des paramètres d'analyseur antivirus personnalisés.
Modifier	Permet de modifier le niveau de protection existant.

- 6 Si vous choisissez de modifier ou de changer les paramètres de l'analyseur, sous **Nom de l'instance**, saisissez un nom unique pour l'instance de paramètre de l'analyseur antivirus. Ce champ est obligatoire.
- 7 Sous l'onglet **Options de base**, sous **Spécifier les fichiers à analyser**, sélectionnez l'une des options suivantes :

Tableau 5-12 Définition des options – Options de base

Option	Définition
Analyser tous les fichiers	Permet d'analyser tous les fichiers, quel que soit leur type.
Types de fichier par défaut	Permet d'analyser seulement les types de fichier par défaut.
Types de fichier par défaut	Permet d'analyser seulement les types de fichier définis. Tapez une extension de fichier à trois lettres. Les extensions de fichiers plus longues sont incluses à l'aide de la correspondance de modèles afin que « cla » corresponde aux fichiers « .class ». Cliquez sur Ajouter . Toutes les extensions en minuscules sont basculées en majuscules.
 Vous pouvez saisir autant de types de fichiers que nécessaire.	

- 8 Sélectionnez d'autres options d'analyseur sous **Options de l'analyseur**. Vous pouvez sélectionner :

Tableau 5-13 Définition des options – Options de l'analyseur


Option	Définition
Analyser des fichiers d'archives (ZIP, ARJ, RAR...)	Permet d'analyser le contenu des fichiers d'archives, comme les fichiers ZIP.
Détecter les virus de fichiers inconnus	Permet d'utiliser des techniques d'analyse heuristique pour rechercher des virus inconnus.
Détecter les virus de macros inconnus	Permet de rechercher des virus inconnus dans les macros.
Activer le service de réputation des fichiers de McAfee Global Threat Intelligence	<p>Permet d'exploiter les informations sur les menaces recueillies par McAfee Avert Labs afin d'éviter des dommages et le vol de données avant même qu'une mise à jour des signatures ne soit disponible. Sélectionnez le niveau de sensibilité. Les options suivantes sont disponibles :</p> <ul style="list-style-type: none"> • Très faible — Équivalent aux DAT des jours suivants. Bénéficiez dès aujourd'hui de la protection de demain. Configuration initiale recommandée. • Faible — Protection en plus des DAT. • Moyenne — Protection utilisée lorsque le risque d'exposition standard à des logiciels malveillants est supérieur au risque de faux positif. • Élevée — Recommandée pour une utilisation dans les référentiels SharePoint qui sont régulièrement infectés. • Très élevée — Recommandée pour une utilisation dans les analyses à la demande sur les référentiels SharePoint. <p> Cette option doit être désactivée si le système n'est pas directement connecté à l'Internet ; autrement, cela peut nuire de façon importante aux performances.</p>
Rechercher les macros dans tous les fichiers	Permet de rechercher les macros dans tous les fichiers.

Tableau 5-13 Définition des options — Options de l'analyseur (suite)

Option	Définition
Rechercher toutes les macros et les considérer comme infectées	Permet de rechercher les macros dans tous les fichiers et de les traiter comme des éléments infectés.
Supprimer toutes les macros des fichiers de documents	Permet de supprimer toutes les macros des fichiers de documents.

9 Sous l'onglet **Avancé**, sous **Catégories personnalisées de programmes malveillants**, spécifiez les éléments à traiter comme des programmes malveillants. Il existe deux manières de sélectionner les types de programme malveillant :

- Sélectionnez les types de programmes malveillants dans la liste de cases à cocher.
- Sélectionnez **Noms de détection spécifiques**, tapez une catégorie de logiciel malveillant, puis cliquez sur **Ajouter**.



Lors de la saisie d'un nom de catégorie de logiciel malveillant, vous pouvez utiliser des caractères génériques pour la recherche.

10 Sélectionnez l'option **Ne pas effectuer de recherche personnalisée de logiciels malveillants si l'objet a déjà été nettoyé**, si les éléments nettoyés ne doivent pas être soumis au contrôle de logiciel malveillant personnalisé.

11 Sous **Options de nettoyage**, spécifiez ce qui arrive aux fichiers qui sont réduits à zéro octet après avoir été nettoyés. Sélectionnez l'une des options suivantes :

- **Garder le fichier d'une taille de zéro octet** — Permet de conserver les fichiers réduits à zéro octet après l'opération de nettoyage.
- **Supprimer le fichier d'une taille de zéro octet** — Permet de supprimer les fichiers réduits à zéro octet après l'opération de nettoyage.
- **Considérer que le nettoyage a échoué** — Permet de considérer les fichiers réduits à zéro octet comme des fichiers qui ne peuvent pas être nettoyés et d'appliquer l'action définie pour les échecs de nettoyage.

12 Sous l'onglet **Packers**, sélectionnez les options suivantes :

- **Activer la détection** — Permet d'activer ou de désactiver la détection des programmes de compression.
- **Exclure les noms spécifiés** — Permet de spécifier les programmes de compression qui peuvent être exclus de l'analyse.
- **Inclure uniquement les noms spécifiés** — Permet de spécifier les programmes de compression qui doivent être détectés par le logiciel.
- **Ajouter** — Permet d'ajouter des noms de programmes de compression à une liste. Vous pouvez utiliser des caractères génériques pour trouver des noms.
- **Supprimer** — Pour supprimer les noms des programmes de compression que vous avez ajoutés. Ce lien est activé si vous cliquez sur **Ajouter**.

13 Sous l'onglet **Programme potentiellement indésirable**, sélectionnez les options suivantes :

- **Activer la détection** — Permet d'activer ou de désactiver la détection des programmes potentiellement indésirables. Cliquez sur le lien de clause d'exclusion de responsabilité et lisez la clause avant de configurer la détection de programmes potentiellement indésirables.
- **Sélectionner les types de programmes à détecter** — Permet de définir, pour chaque type de programme potentiellement indésirable dans la liste, s'il doit être détecté ou ignoré.

- **Exclure les noms spécifiés** — Permet de spécifier les programmes potentiellement indésirables qui peuvent être exclus de l'analyse. Par exemple, si vous avez activé la détection des logiciels espions (spyware), vous pouvez créer une liste de ces programmes que le logiciel doit ignorer.
- **Inclure uniquement les noms spécifiés** — Permet de spécifier les programmes potentiellement indésirables que le logiciel doit détecter. Par exemple, si vous activez la détection des logiciels espions et que vous spécifiez que seuls les programmes espions nommés doivent être détectés, tous les autres programmes espions seront ignorés.
- **Ajouter** — Permet d'ajouter les noms de programmes potentiellement indésirables à une liste. Vous pouvez utiliser des caractères génériques pour trouver des noms.
- **Supprimer** — Permet de supprimer les noms de programmes potentiellement indésirables que vous avez ajoutés. Ce lien est activé si vous cliquez sur **Ajouter**.



Le site web de [McAfee Threat Intelligence](#) met à disposition une liste des noms de logiciels malveillants (malware) récents. Pour afficher des informations sur un programme malveillant précis, utilisez la section **Search the Threat Library** (Rechercher dans la bibliothèque de menaces).

- 14 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 15 Sous **Actions à entreprendre**, cliquez sur **Modifier**. Sous les onglets suivants, spécifiez les actions d'analyseur antivirus à prendre si un virus (ou un comportement de type viral) est détecté.
- 16 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.
- 17 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres de filtrage de fichiers

Configurez les paramètres dans une stratégie afin de détecter les fichiers en fonction de leur nom, de leur type ou de leur taille et d'entreprendre les actions nécessaires correspondantes.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant l'analyseur **Filtrage des fichiers**.
La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Filtrage des fichiers**.
- 4 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de l'analyseur de filtrage de fichiers correspondant à l'élément de sous-menu choisi.



Si vous êtes en train de configurer les paramètres d'une sous-stratégie, sélectionnez l'option **Utiliser la configuration de la stratégie parente** afin d'hériter des paramètres de la stratégie parente.

5 Sous **Sélection d'alerte**, cliquez sur :

- **Créer** — Permet de créer un nouveau message d'alerte lorsque le document sur le serveur SharePoint est remplacé suite au déclenchement d'une règle. Pour obtenir des instructions, consultez la section *Création d'une nouvelle alerte*.
- **Afficher/Masquer** — Permet d'afficher ou de masquer le texte du message d'alerte. Si l'aperçu est masqué, cliquez sur ce lien pour l'afficher. Si l'aperçu est affiché, cliquez sur ce lien pour le masquer.



Vous pouvez créer des alertes uniquement pour les stratégies à la demande.

6 Sous **Règles de filtrage des fichiers et actions associées**, dans le menu déroulant **Règles disponibles**, sélectionnez une règle disponible. Si vous souhaitez créer des règles de filtrage de fichiers, sélectionnez **<Créer une nouvelle règle...>**. Pour obtenir des instructions complémentaires sur la création de règles de filtrage de fichiers, consultez la section *Configuration des règles de filtrage de fichiers*.

7 Cliquez sur **Modifier** pour spécifier les actions qui doivent être prises quand un élément déclenche l'analyseur.

8 Cliquez sur **Supprimer** pour supprimer une règle existante de la stratégie.

9 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres d'analyseur de conformité et DLP

Configurez les paramètres de l'**Analyseur de conformité et DLP** dans une stratégie afin d'identifier les données des documents ou autres éléments non conformes et prendre les mesures nécessaires correspondantes.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant l'analyseur **Conformité et DLP**.

La page de stratégie relative à l'élément de sous-menu s'affiche.

2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.

3 Cliquez sur **Analyseur de conformité et DLP**.

4 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de l'analyseur de conformité et DLP correspondant à l'élément de sous-menu choisi.



- Par défaut, toutes les options de configuration de l'analyseur sont désactivées pour l'**Analyseur de conformité et DLP** pour ces sous-stratégies.
- Si vous êtes en train de configurer les paramètres d'une sous-stratégie, sélectionnez l'option **Utiliser la configuration de la stratégie parente** afin d'hériter des paramètres de la stratégie parente.

5 Sous **Options**, vous pouvez utiliser les options suivantes :

- **Inclure les formats de document et de base de données** : permet d'analyser les documents et formats de base de données à la recherche de contenu non conforme.
- **Analyser le texte de toutes les pièces jointes** — Permet d'analyser le texte de toutes les pièces jointes.

- **Créer** — Permet de créer un nouveau message d'alerte lorsque le contenu d'un élément est remplacé suite au déclenchement d'une règle. Pour obtenir des instructions, consultez la section *Création d'une nouvelle alerte*.
- **Afficher/Masquer** — Permet d'afficher ou de masquer le texte du message d'alerte. Si l'aperçu est masqué, cliquez sur ce lien pour l'afficher. Si l'aperçu est affiché, cliquez sur ce lien pour le masquer.

6 Sous **Règles de conformité et DLP, et actions associées**, cliquez sur **Ajouter une règle**.

La page **Règles de conformité et DLP** s'affiche.

7 Sous **Spécifier les actions à associer à la règle**, dans le menu déroulant **Sélectionner un groupe de règles**, sélectionnez un groupe de règles qui déclenchera une action si une ou plusieurs de ses règles ne sont pas respectées. Chaque expression peut se voir attribuer un **Score** pour une catégorie donnée, sous **Expression de l'analyseur de conformité et DLP**.

Pour certains groupes de règles, il peut s'avérer nécessaire de configurer les options suivantes :

- **Seuil du score** — Permet de spécifier le seuil de score maximum de déclenchement de l'analyseur.
- **Nombre max. de termes** — Permet de spécifier le nombre de déclenchements maximal de ce groupe de règles. En cas de dépassement de ce nombre, l'analyseur entreprend l'action indiquée.

L'équation **Seuil du score** = **Score** x nombre de termes (d'instances). Une règle se déclenche lorsque la valeur est supérieure ou égale à celle définie pour **Seuil du score**.

Pour comprendre l'intérêt que présentent les options **Seuil du score** et **Nombre max. de termes** dans le déclenchement d'une règle, prenons un exemple tiré du dictionnaire de langage Pascal. Supposons que l'option **Score** définie pour l'**Expression de l'analyseur de conformité et DLP** « PAnsiChar » soit configurée sur 5.

Sous **Sélectionner un groupe de règles**, supposons que vous ayez sélectionné le dictionnaire **Pascal Language** (Langage Pascal) et attribué les valeurs suivantes :

- **Seuil du score** = 15
- **Nombre max. de termes** = 4

Si deux occurrences de « PAnsiChar » figurent dans le code, le seuil de score est égal à 10. Par conséquent, la règle ne se déclenche PAS.

Si cinq occurrences de « PAnsiChar » sont identifiées dans le code, le score actuel est toujours calculé selon la formule **Score** x **Nombre max. de termes**, ce qui équivaut à $5 * 4 = 20$. Cette valeur est supérieure au seuil de score défini. Dans ce cas, la règle se déclenche.

Supposons que vous ayez attribué au **Score** de l'expression « PAnsiChar » la valeur 8. Si l'expression « PAnsiChar » apparaît trois fois dans le code, le seuil de score actuel est égal à 24. Dans ce cas, la règle se déclenche, car elle dépasse la valeur spécifiée pour l'option **Seuil du score**.

Si plusieurs règles sont définies, l'option **Seuil du score** correspond à la valeur combinée de toutes les règles définies pour un dictionnaire.



Une règle se déclenche uniquement lorsque la valeur est supérieure ou égale à celle de l'option **Seuil du score** et elle ne se déclenche pas même si l'instance de l'expression dépasse la valeur de l'option **Nombre max. de termes** dans un document.

8 Sous **En cas de détection, entreprendre l'action suivante** :, sélectionnez les actions d'analyseur de conformité et DLP à entreprendre si un contenu non conforme est détecté dans un élément.

- 9 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.
- 10 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Gestion des paramètres de filtre associés à une stratégie

Activez ou désactivez les options de filtre, puis spécifiez une action appropriée à entreprendre concernant l'élément détecté suite au déclenchement d'une stratégie.

Les filtres disponibles sont les suivants :

- Contenu corrompu
- Contenu protégé
- Contenu crypté
- Contenu signé
- Fichiers protégés par mot de passe
- Contrôle de l'analyseur

Procédures

- [Configuration des paramètres de contenu corrompu, page 70](#)
Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu corrompu et de prendre les mesures nécessaires correspondantes.
- [Configuration des paramètres de contenu protégé, page 71](#)
Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu protégé et de prendre les mesures nécessaires correspondantes.
- [Configuration des paramètres de contenu chiffré, page 71](#)
Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu chiffré et de prendre les mesures nécessaires correspondantes.
- [Configuration des paramètres de contenu signé, page 72](#)
Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu signé et de prendre les mesures nécessaires correspondantes.
- [Configuration des paramètres des fichiers protégés par mot de passe, page 73](#)
Configurez les paramètres dans une stratégie afin d'identifier les éléments protégés par mot de passe et de prendre les actions nécessaires correspondantes.
- [Configuration des paramètres de contrôle de l'analyseur, page 73](#)
Configurez les paramètres dans une stratégie qui définit le niveau d'imbrication, la taille du fichier décompressé et la durée d'analyse maximale autorisée lors de l'analyse des éléments.

Configuration des paramètres de contenu corrompu

Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu corrompu et de prendre les mesures nécessaires correspondantes.

Le contenu de certains documents peut devenir corrompu et impossible à analyser. Les stratégies de contenu corrompu déterminent le mode de gestion des éléments en cas de détection d'un contenu corrompu.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant le filtre.
La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.

- 3 Cliquez sur **Contenu corrompu**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.
- 5 Dans **Actions**, cliquez sur **Modifier** pour indiquer les actions de filtre qui doivent être entreprises lors de la détection de contenu altéré.



Cliquez sur **Réinitialiser** pour rétablir les valeurs par défaut dans **Actions de contenu altéré**.

- 6 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 7 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres de contenu protégé

Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu protégé et de prendre les mesures nécessaires correspondantes.

Les stratégies de contenu protégé déterminent le mode de gestion des éléments en cas de détection d'un contenu protégé.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant le filtre.
La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Contenu protégé**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.
- 5 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions de filtre qui doivent être entreprises lors de la détection de contenu protégé.



Cliquez sur **Réinitialiser** pour rétablir les valeurs par défaut dans **Actions de contenu protégé**.

- 6 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 7 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres de contenu chiffré

Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu chiffré et de prendre les mesures nécessaires correspondantes.

Vous avez la possibilité de chiffrer des documents afin d'empêcher les parties non autorisées d'y accéder. Le Contenu chiffré fait appel à une clé et à des algorithmes mathématiques de chiffrement pour la déchiffrer. Les stratégies de contenu chiffré déterminent le mode de gestion des éléments en cas de détection d'un contenu chiffré.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant le filtre.
La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Contenu crypté**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.



Les paramètres du contenu chiffré sont activés par défaut.

- 5 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions de filtre qui doivent être entreprises lors de la détection de contenu chiffré.



Cliquez sur **Réinitialiser** pour rétablir les valeurs par défaut dans **Actions de contenu crypté**.

- 6 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 7 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres de contenu signé

Configurez les paramètres dans une stratégie afin d'identifier les éléments au contenu signé et de prendre les mesures nécessaires correspondantes.

Les stratégies de contenu signé déterminent le mode de gestion des éléments en cas de détection d'un contenu signé.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant le filtre.
La page de stratégie relative à l'élément de sous-menu s'affiche.
- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Contenu signé**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.
- 5 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions de filtre qui doivent être entreprises lors de la détection de contenu signé.



Cliquez sur **Réinitialiser** pour rétablir les valeurs par défaut dans **Actions de contenu signé**.

- 6 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 7 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres des fichiers protégés par mot de passe

Configurez les paramètres dans une stratégie afin d'identifier les éléments protégés par mot de passe et de prendre les actions nécessaires correspondantes.

Il est impossible d'accéder aux fichiers protégés par mot de passe et de les analyser sans mot de passe. Les stratégies protégées par mot de passe précisent comment ces éléments doivent être traités une fois qu'ils ont été détectés.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant le filtre.

La page de stratégie relative à l'élément de sous-menu s'affiche.

- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Contenu protégé par mot de passe**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.
- 5 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions de filtre à prendre.



Cliquez sur **Réinitialiser** pour rétablir les valeurs par défaut dans **Actions de contenu protégé par mot de passe**.

- 6 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.
- 7 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

Configuration des paramètres de contrôle de l'analyseur

Configurez les paramètres dans une stratégie qui définit le niveau d'imbrication, la taille du fichier décompressé et la durée d'analyse maximale autorisée lors de l'analyse des éléments.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de sous-menu désignant l'analyseur.

La page de stratégie relative à l'élément de sous-menu s'affiche.

- 2 Cliquez sur **Stratégie principale** ou sur une sous-stratégie à configurer, puis sur l'onglet **Afficher la liste de tous les analyseurs**.
- 3 Cliquez sur **Contrôle de l'analyseur**.
- 4 Pour une sous-stratégie, cliquez sur **Utiliser la configuration de la stratégie parente** afin d'hériter de tous les paramètres de la stratégie parente.
- 5 Sous **Options**, cliquez sur **<créer un nouveau jeu d'options>**.
- 6 Dans **Nom de l'instance**, tapez un nom unique pour l'instance de configuration du filtre de contrôle de l'analyseur. Ce champ est obligatoire.
- 7 Dans le champ **Niveau maximal d'imbrication**, spécifiez le niveau auquel l'analyseur doit opérer lorsqu'une pièce jointe contient des fichiers compressés et d'autres fichiers compressés à l'intérieur. Vous pouvez indiquer une valeur comprise entre 2 et 100, la valeur par défaut étant 100.

8 Dans le champ **Taille maximale du fichier décompressé (Mo)**, spécifiez la taille maximale qu'un fichier peut atteindre une fois décompressé pour l'analyse. Vous pouvez indiquer une valeur comprise entre 1 et 2 047, la valeur par défaut étant 500.

Le champ **Durée maximale d'analyse (minutes)** indique la durée maximale autorisée pour l'analyse d'un fichier. Cette valeur provient des paramètres d'antivirus Sharepoint.

9 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.

10 Sous **Sélection d'alerte**, vous pouvez sélectionner l'alerte à utiliser lorsqu'une option de contrôle de l'analyseur est déclenchée. Vous pouvez utiliser les options suivantes :

- **Créer** — Permet de créer un nouveau message d'alerte pour cette stratégie.
- **Afficher/Masquer** — Permet d'afficher ou de masquer le texte d'alerte. Si le texte est masqué, cliquez sur le lien pour l'afficher. S'il est affiché, cliquez sur le lien pour le masquer.

11 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions à prendre, si la valeur dépasse les paramètres spécifiés pour le niveau maximal d'imbrication, la taille maximum du fichier décompressé et la durée maximale d'analyse.

12 Cliquez sur **Enregistrer** pour revenir à la page de stratégie.

13 Cliquez sur **Appliquer** pour configurer ces paramètres dans une stratégie.

6

Paramètres et diagnostics

Permet la configuration de l'activation, la désactivation, la configuration et l'administration des fonctionnalités et des journaux associés pour le logiciel en fonction des stratégies de sécurité de votre organisation.

Pour modifier ou afficher les paramètres du produit, cliquez sur **Paramètres et diagnostics** dans l'interface utilisateur du produit. Ce tableau explique brièvement les situations dans lesquelles il est opportun de configurer ces paramètres :

Tableau 6-1 Paramètres et diagnostics

Paramètres	Objectif
Éléments détectés	Permet de configurer et gérer les activités de la base de données de quarantaine locale comme la purge et l'optimisation. Des options permettent également de spécifier la taille de l'élément, la taille de la requête et l'âge de l'élément.
Préférences de l'interface utilisateur	Configurez les paramètres disponibles dans le Tableau de bord , notamment la fréquence d'actualisation, les paramètres de rapport, les unités de l'échelle du graphique, l'intervalle de génération de rapports, et les paramètres des graphiques et diagrammes.
Diagnostics	Définissez les paramètres relatifs au débogage, à la notification d'erreurs ainsi qu'aux journaux du produit et aux événements, notamment les informations sur la taille et l'emplacement d'enregistrement des journaux. Les paramètres de diagnostics sont les suivants : <ul style="list-style-type: none">• Consignation du débogage• Service de rapport d'erreurs• Journalisation des événements• Journal du produit
Journal du produit	Permet de consulter le Journal du produit et de filtrer la sortie par date, type ou description.
Importer et exporter la configuration	Configurez votre serveur actuel du produit avec les mêmes configurations que celles qui sont déjà créées, restaurez les paramètres par défaut ou créez des fichiers Sitelist pointant vers les emplacements de téléchargement des fichiers DAT.

Tableau 6-1 Paramètres et diagnostics (suite)

Paramètres	Objectif
Paramètres de DAT	Permet de spécifier le nombre maximum de fichiers de signatures de détection à conserver à la place des fichiers DAT.
Paramètres utilisateur	<p>Permet de définir la procédure à appliquer à un élément quand l'analyseur ne parvient pas à analyser un élément lors d'une analyse à l'accès. Les options sont les suivantes :</p> <ul style="list-style-type: none"> • Autoriser • Empêcher le chargement <p>Fournit d'autres options permettant de spécifier l'intervalle analyseur, le nombre d'analyseurs et la taille de la zone de quarantaine Sharepoint, ainsi que l'ajout de pools d'applications.</p>

Si vous modifiez l'un de ces paramètres, veillez à cliquer sur **Appliquer** pour enregistrer les modifications. La couleur d'arrière-plan du bouton **Appliquer** devient :



- jaune si vous avez modifié un paramètre existant ou que la modification n'est pas encore appliquée.
- verte si vous n'avez pas modifié de paramètre existant ou que la modification est appliquée.

Sommaire

- ▶ *Configurer la base de données de quarantaine locale pour les éléments détectés*
- ▶ *Paramètres des préférences de l'interface utilisateur*
- ▶ *Paramètres de diagnostics*
- ▶ *Affichage des journaux du produit*
- ▶ *Importation et exportation de paramètres de configuration*
- ▶ *Configuration des paramètres de fichiers DAT*
- ▶ *Configuration des paramètres utilisateur*

Configurer la base de données de quarantaine locale pour les éléments détectés

Spécifiez les paramètres de référentiel pour le stockage des éléments mis en quarantaine détectés par le logiciel.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Éléments détectés**.

La page **Éléments détectés** s'affiche.

- 2 A partir de la section **Base de données locale**, vous pouvez utiliser les options suivantes :

Tableau 6-2 Définition des options





Option	Définition
Spécifier l'emplacement de la base de données	Pour changer l'emplacement de la base de données de stockage des éléments mis en quarantaine détectés par le logiciel. Le <Dossier d'installation> est l'emplacement par défaut de la base de données.
Emplacement de la base de données	<p>Permet de spécifier le chemin d'accès à l'emplacement de la base de données dans laquelle les éléments détectés par le logiciel peuvent être stockés. Vous pouvez sélectionner :</p> <ul style="list-style-type: none"> • <Dossier d'installation> : permet de créer les sous-dossiers de la base de données sous le répertoire d'installation du produit. • <Lecteur système> : permet de créer les sous-dossiers de la base de données sous le répertoire C:\ du lecteur d'installation du système d'exploitation. • <Fichiers programme> : permet de créer les sous-dossiers de la base de données sous le répertoire Windows C:\Program Files (x86). • <Dossier Windows> : permet de créer les sous-dossiers de la base de données sous le répertoire C:\Windows. • <Chemin d'accès complet> : permet de spécifier le chemin d'accès complet de la base de données locale. <p> Spécifiez le chemin d'accès au sous-dossier dans le champ situé en regard de la liste déroulante.</p>
Taille maximale de l'élément (Mo)	<p>Permet de spécifier la taille maximale que peut atteindre un élément mis en quarantaine pour être stocké dans la base de données. Vous pouvez indiquer une valeur comprise entre 1 et 100, la valeur par défaut étant 100.</p> <p> Si la taille maximale de l'élément est supérieure à 100, il ne sera alors pas mis en quarantaine.</p>
Taille maximale de la requête (enregistrements)	Permet de spécifier le nombre maximal d'enregistrements ou d'éléments mis en quarantaine que vous pouvez interroger à partir de la page Éléments détectés . Vous pouvez indiquer une valeur comprise entre 1 et 20 000, la valeur par défaut étant 1 000.
Age maximal de l'élément (jours)	Permet de spécifier le nombre maximal de jours pendant lequel un élément peut être conservé dans la base de données de quarantaine locale avant d'être marqué pour la suppression. Vous pouvez indiquer une valeur comprise entre 1 et 365, la valeur par défaut étant 14.
Fréquence de purge des éléments anciens	<p>Permet de spécifier la fréquence à laquelle les anciens éléments marqués pour la suppression sont retirés de la base de données du produit. La valeur par défaut est Quotidienne.</p> <p> Pour plus d'informations sur le retrait des anciens éléments marqués pour la suppression, consultez <i>Purge et optimisation</i>.</p>

Tableau 6-2 Définition des options (suite)

Option	Définition
Fréquence d'optimisation	<p>Permet de récupérer l'espace disque occupé par les enregistrements de base de données supprimés. En fonction de la valeur définie sous Age maximal de l'élément (jours), les anciens enregistrements seront supprimés si vous avez planifié une tâche de purge. Afin d'optimiser et de réduire la base de données, planifiez une tâche d'optimisation. La valeur par défaut est ///Not scheduled.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Pensez à toujours planifier une tâche d'optimisation quelques heures après avoir effectué une tâche de purge.</p> <p>Pour plus d'informations sur le retrait des anciens éléments marqués pour la suppression, consultez <i>Purge et optimisation</i>.</p> </div>
Modifier la planification	<p>Permet de modifier la planification de la tâche de purge ou d'optimisation. Cliquez sur Enregistrer après avoir modifié la planification.</p>

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez correctement configuré le serveur du produit pour l'application de la mise en quarantaine des éléments détectés dans la base de données locale.

Paramètres des préférences de l'interface utilisateur

Configurez les paramètres disponibles dans le **Tableau de bord**, notamment la fréquence d'actualisation, les paramètres de rapport, les unités de l'échelle du graphique, l'intervalle de génération de rapports, et les paramètres des graphiques et diagrammes.

Configuration des paramètres du tableau de bord

Configurez les paramètres du **Tableau de bord**, notamment les statistiques, les unités de l'échelle du graphique, les éléments à afficher sous **Éléments récemment analysés**, ainsi que l'intervalle de rapport de statut.

Procédure


Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Préférences de l'interface utilisateur**.

La page **Préférences de l'interface utilisateur** s'affiche.

- 2 Cliquez sur l'onglet **Paramètres du tableau de bord**. Vous pouvez utiliser les options suivantes :

Tableau 6-3 Définition des options

Option	Définition
Actualisation automatique	Permet de spécifier si les informations affichées dans le compteur Tableau de bord Statistiques doivent s'actualiser automatiquement.  Veillez à ce que cette option soit toujours activée si vous voulez voir les statistiques actualisées du tableau de bord.
Fréquence d'actualisation (secondes)	Permet de spécifier la périodicité (en secondes) à laquelle les informations doivent être actualisées sur le tableau de bord. Vous pouvez indiquer une valeur comprise entre 30 et 3 600, la valeur par défaut étant 60.
Nombre maximal d'éléments analysés récemment	Permet de spécifier le nombre maximal d'éléments devant s'afficher dans la section Tableau de bord Rapports Eléments récemment analysés . Vous pouvez indiquer une valeur comprise entre 10 et 100, la valeur par défaut étant 20.
Echelle du graphique (unités)	Permet de spécifier les unités de mesure de l'échelle du graphique à barres généré dans la section Tableau de bord Graphique . Vous pouvez indiquer une valeur comprise entre 100 et 500, la valeur par défaut étant 100.
Nombre d'heures dont les données doivent être affichées	Permet de spécifier l'intervalle de génération entre deux rapports en heures. Vous pouvez indiquer une valeur comprise entre 1 et 24, la valeur par défaut étant 7.

- 3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration des paramètres des graphiques et diagrammes

Configurez les paramètres de la section **Tableau de bord | Graphique** en vue d'améliorer les paramètres des graphiques et diagrammes.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Préférences de l'interface utilisateur**.
- 2 Cliquez sur l'onglet **Paramètres des graphiques et diagrammes**. Vous pouvez utiliser les options suivantes :

Tableau 6-4 Définition des options

Option	Définition
3D	Permet d'afficher le graphique du tableau de bord en trois dimensions (3D).
Tracer le transparent	Permet d'indiquer si les barres d'un graphique à barres en 3D doivent être visibles ou transparentes. Les barres pleines cachent en partie les barres qu'elles recouvrent. Les barres transparentes permettent de voir les autres barres transparentes qu'elles recouvrent.
Anticrénelage	Permet d'utiliser les techniques d'anticrénelage pour l'affichage des graphiques à secteurs. Si l'anticrénelage est utilisé, les courbes des graphiques à secteurs sont adoucies. Sinon, leurs courbes sont plus dentelées.
Graphique à secteurs	Permet d'indiquer si les segments doivent rester à l'intérieur du cercle du graphique à secteurs ou être affichés sous forme de segments décomposés.
Angle de secteur (degrés)	Permet de spécifier l'angle à appliquer pour l'affichage des graphiques à secteurs. Vous pouvez indiquer une valeur comprise entre 1 et 360, la valeur par défaut étant 45.

- 3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Paramètres de diagnostics

Déterminez les causes de symptômes et les erreurs rencontrées lors de l'utilisation de McAfee Security for Microsoft SharePoint.

La page **Paramètres et diagnostics | Diagnostics** vous propose les options suivantes :

- **Consignation du débogage** : permet de configurer les paramètres de journalisation de débogage, notamment de spécifier le niveau de journalisation de débogage, la taille maximale du fichier journal ainsi que l'emplacement du fichier.
- **Service de rapport d'erreurs** : permet de configurer les paramètres de détection des exceptions (telles que les blocages système).
- **Journalisation des événements** : permet de configurer les paramètres de capture des journaux relatifs au produit ou aux événements en fonction des informations, des avertissements ou des erreurs.
- **Journal du produit** : permet de configurer les paramètres relatifs au fichier du journal du produit (`productlog.bin`). Les modifications apportées à ce paramètre sont ensuite répercutées sur la page **Paramètres et diagnostics | Journal du produit**.

Configuration des paramètres du journal de débogage

Configurez les paramètres permettant de définir le niveau de journalisation de débogage, la taille maximale du fichier journal ainsi que l'emplacement du fichier journal. Servez-vous de ces paramètres pour résoudre un problème relatif au produit et fournir des journaux au Support technique McAfee à des fins d'analyse ultérieure.



Configurez les paramètres du **journal de débogage** à des fins de dépannage et pour une durée limitée uniquement. Dès lors que vous avez capturé suffisamment de journaux pour le dépannage, attribuez la valeur **Niveau** sur **Aucun**. L'utilisation de la journalisation de débogage sans discrimination risque de saturer l'espace disque et d'affecter les performances globales du serveur. Activez-la pour une durée limitée, sur les conseils d'un agent agréé (membre du Support technique McAfee).

Procédure



Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Diagnostics**.

La page **Diagnostics** s'affiche.

- 2 Sous l'onglet **Consignation du débogage**, vous pouvez utiliser les options suivantes :

Tableau 6-5 Définition des options

Option	Définition
Niveau	<p>Permet d'activer ou de désactiver la journalisation de débogage et de préciser le niveau d'informations à capturer dans le fichier journal de débogage. Vous pouvez sélectionner :</p> <ul style="list-style-type: none"> • Aucun : permet de désactiver la journalisation de débogage. • Faible : permet de consigner dans le fichier journal de débogage des événements critiques tels que des erreurs, des exceptions et des valeurs de retour de fonctions. Sélectionnez cette option pour conserver une taille minimale de fichier journal de débogage. • Moyen — Permet de consigner les événements mentionnés sous l'état Faible et d'autres informations pouvant aider l'équipe de support technique. • Elevé : permet de consigner dans le fichier journal de débogage l'ensemble des erreurs critiques, avertissements et messages de débogage. Ce fichier contient alors des informations sur toutes les activités exécutées par le produit. Il s'agit du niveau de journalisation le plus détaillé pris en charge par le produit.
Activer la limite de taille	Permet de spécifier une taille de fichier maximale pour chaque fichier journal de débogage.
Taille de fichier maximale	<p>Permet de spécifier la taille maximale des fichiers journaux de débogage. Vous pouvez indiquer une valeur comprise entre 1 Ko et 2 000 Mo.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Si les fichiers journaux de débogage dépassent la taille fixée, les événements les plus anciens sont écrasés suivant le principe de la journalisation circulaire, selon lequel les nouvelles entrées de journal sont ajoutées au fichier en supprimant les plus anciennes.</p> </div>
Activer la journalisation de débogage	Permet de modifier l'emplacement par défaut de journalisation des fichiers de débogage.
Emplacement du fichier	<p>Permet de spécifier le chemin d'accès à l'emplacement du fichier journal de débogage où les événements déclenchés par le produit peuvent être stockés. Vous pouvez sélectionner :</p> <ul style="list-style-type: none"> • <Bureau> : permet de créer les fichiers journaux de débogage sur le bureau. • <Dossier d'installation> : permet de créer les fichiers journaux de débogage sous le répertoire d'installation du produit. • <Lecteur système> — permet de créer les sous-dossiers de la base de données sous le répertoire C:\ du lecteur d'installation du système d'exploitation. • <Fichiers programme> : permet de créer les sous-dossiers de la base de données sous le répertoire Windows C:\Program Files (x86). • <Dossier Windows> : permet de créer les fichiers journaux de débogage sous le répertoire C:\Windows. • <Chemin d'accès complet> : permet de stocker les fichiers journaux de débogage dans le chemin d'accès complet spécifié dans la zone de texte adjacente. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Pour stocker les fichiers journaux de débogage à un emplacement personnalisé ou dans un sous-dossier précis, spécifiez cet emplacement ou le nom de ce sous-dossier dans le champ situé en regard de la liste déroulante.</p> </div>



Assurez-vous que le dossier qui collecte les journaux de débogage dispose d'autorisations en écriture sur le compte SERVICE RESEAU.

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez à présent terminé la configuration des paramètres de journalisation de débogage, que vous pouvez utiliser pour résoudre des problèmes.

Configuration des paramètres de génération de rapports d'erreur McAfee

Configurez les paramètres de génération de rapports sur les erreurs ou exceptions liées au produit à transmettre à McAfee.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Diagnostics**.

La page **Diagnostics** s'affiche.

2 Cliquez sur l'onglet **Service de notification d'erreurs**. Vous pouvez utiliser les options suivantes :

Tableau 6-6 Définition des options

Option	Définition
Activer	Permet d'activer ou de désactiver le service de génération de rapports d'erreur.
Détecter les exceptions	Permet de capturer des informations sur les événements qui génèrent des exceptions.
Signaler les exceptions à l'utilisateur	Permet d'indiquer si les exceptions doivent faire l'objet d'un rapport destiné à l'administrateur.

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration des paramètres du journal d'événements

Configurez les paramètres pour consigner les événements du produit dans le **Journal du produit** et l'Observateur d'événements Windows.

Un événement désigne une action que vous pouvez effectuer et qui est surveillée par le logiciel. La fonctionnalité **Journalisation des événements** fournit des informations utiles pour les diagnostics et les audits. Les différentes classes d'événements sont les suivantes :

- Erreur
- Informations
- Avertissement

Cette fonctionnalité vous permet d'obtenir plus facilement des informations sur les problèmes qui se produisent.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Diagnostics**.

La page **Diagnostics** s'affiche.

2 Cliquez sur l'onglet **Journalisation des événements**. Vous pouvez utiliser les options suivantes :

Tableau 6-7 Définition des options

Option	Définition
Journal du produit	Permet de consigner les événements concernant le produit dans le Journal du produit . Vous pouvez visualiser ces événements à partir de la section Paramètres et diagnostics Journal du produit Afficher les résultats .
Journal des événements	Permet de consigner les événements concernant le produit dans l'Observateur d'événements Windows. Permet de retrouver les événements relatifs au produit dans l'Observateur d'événements Windows : 1 Accédez à Observateur d'événements (local) Journaux Windows Application . 2 Dans le volet Application , les événements relatifs au produit figurent sous l'intitulé McAfee PortalShield de la colonne Source .
Ecrire les événements d'information	Permet de consigner les événements classés dans la catégorie Information .
Ecrire les événements d'avertissement	Permet de consigner les événements classés dans la catégorie Avertissement .
Ecrire les événements d'erreur	Permet de consigner les événements classés dans la catégorie Erreur .

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration des paramètres du journal du produit

Configurez les paramètres du produit en spécifiant les paramètres requis pour générer les journaux du produit.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Diagnostics**.
La page **Diagnostics** s'affiche.
- 2 Cliquez sur l'onglet **Journal du produit**. Vous pouvez utiliser les options suivantes :

Tableau 6-8 Définition des options




Option	Définition
Emplacement	Permet de configurer un emplacement de stockage pour le journal du produit. Sélectionnez Activer pour spécifier un emplacement personnalisé.
Emplacement de la base de données	<p>Permet de spécifier le chemin d'accès à l'emplacement du fichier journal du produit contenant les événements du journal du produit. Vous pouvez sélectionner :</p> <ul style="list-style-type: none"> • <Bureau> : permet de créer les fichiers journaux de débogage sur le bureau. • <Dossier d'installation> : permet de créer les fichiers journaux de débogage sous le répertoire d'installation du produit. • <Lecteur système> : permet de créer les sous-dossiers de la base de données sous le répertoire C:\ du lecteur d'installation du système d'exploitation. • <Fichiers programme> : permet de créer les sous-dossiers de la base de données sous le répertoire Windows C:\Program Files (x86). • <Dossier Windows> : permet de créer les fichiers journaux de débogage sous le répertoire C:\Windows. • <Chemin d'accès complet> : permet de stocker les fichiers journaux de débogage dans le chemin d'accès complet spécifié dans la zone de texte adjacente. <p> Pour stocker le fichier journal du produit à un emplacement personnalisé ou dans un sous-dossier précis, spécifiez cet emplacement ou le nom de ce sous-dossier dans le champ situé en regard de la liste déroulante.</p>
Nom du fichier	Permet de spécifier un nom de fichier différent sous lequel stocker le journal du produit. Sélectionnez Activer pour spécifier un nom de fichier personnalisé.
Nom de fichier de la base de données	<p>Permet de spécifier un nom de fichier personnalisé pour le journal du produit. Le nom de fichier par défaut est <code>productlog.bin</code> sous le répertoire <Dossier d'installation>.</p> <p> Si vous modifiez le nom de fichier ou le chemin d'accès par défaut du journal du produit, les entrées du journal figurant à la page Paramètres et diagnostics Journal du produit seront réinitialisées et les entrées plus anciennes ne seront pas visibles.</p>
Limite de taille	Permet de spécifier une limite de taille différente pour le fichier journal du produit. Sélectionnez Activer la limite de taille de base de données pour spécifier une taille de fichier personnalisée.
Taille de base de données maximale	<p>Permet de spécifier la taille de fichier maximale du journal du produit. Vous pouvez indiquer une valeur comprise entre 1 Ko et 2 000 Mo.</p> <p> Si la taille de fichier du journal du produit dépasse la valeur indiquée, les événements de journal les plus anciens sont écrasés suivant le principe de la journalisation circulaire, selon lequel les nouvelles entrées de journal sont ajoutées au fichier en supprimant les plus anciennes.</p>
Limiter l'âge des entrées	Permet de supprimer les entrées du journal du produit après une période définie.
Age maximal de l'entrée (jours)	Permet de spécifier le nombre de jours pendant lequel une entrée doit rester dans le fichier journal du produit avant d'être supprimée. Vous pouvez indiquer une valeur comprise entre 1 et 365.

Tableau 6-8 Définition des options (suite)

Option	Définition
Délai d'expiration de la requête	Permet de limiter le laps de temps autorisé pour répondre à une requête du journal du produit. Sélectionnez Activer pour spécifier la durée.
Délai d'expiration de la requête (secondes)	Permet de spécifier le laps de temps maximal (exprimé en secondes) autorisé pour répondre à une requête du journal du produit. Vous pouvez indiquer une valeur comprise entre 1 et 3 600.

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez à présent terminé la configuration des paramètres de la page **Journal du produit**.

Affichage des journaux du produit

Affichez l'état de fonctionnement du produit à l'aide des entrées du journal relatives aux niveaux des événements de type informations, avertissements et erreurs. Par exemple, vous pouvez visualiser des informations sur la progression d'une tâche (lancée ou terminée), les erreurs de service relatives au produit, etc.

Les filtres de recherche disponibles permettent d'identifier les entrées de journal qui vous intéressent.



Pour modifier les paramètres relatifs à la page de requête de journal du produit, accédez à **Paramètres et diagnostics | Diagnostics | Journal du produit**.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Journal du produit**. La page **Journal du produit** s'affiche.
- 2 Dans la section **Journal du produit**, vous pouvez utiliser les options suivantes :

Tableau 6-9 Définition des options

Option	Définition
ID	Permet d'indiquer le numéro servant à identifier une entrée spécifique du journal du produit.
Niveau	Permet de sélectionner Information , Avertissement ou Erreur dans la liste déroulante, selon le type de journal à afficher.
Description	Permet de fournir une description pertinente. Par exemple, si vous souhaitez afficher les journaux en fonction du démarrage ou de l'arrêt du service, saisissez : <code>*service*</code>
Toutes les dates	Permet d'inclure les événements englobant toutes les dates, en fonction de l'entrée dans le fichier journal du produit.
Plage de dates	Permet de rechercher un événement dans une plage de dates définie conformément à vos exigences. Cette option vous permet de spécifier la date, le mois, l'année et l'heure de comparaison par rapport aux paramètres De et A . Vous pouvez également spécifier une plage de dates à l'aide de l'icône de calendrier.
Effacer le filtre	Permet de rétablir les paramètres de recherche par défaut.

Tableau 6-9 Définition des options (suite)

Option	Définition
Exporter vers un fichier .CSV	<p>Permet d'exporter et d'enregistrer des informations concernant tous les événements renvoyés par la recherche au format .CSV. Si le journal comprend des milliers d'événements, vous pouvez, plutôt que de parcourir plusieurs pages, utiliser cette option pour télécharger ces événements dans un fichier au format CSV et générer par la suite des rapports personnalisés dans Microsoft Excel.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> • Si un champ donné est introuvable dans le résultat de la recherche du fichier CSV, veillez à activer le champ requis sous l'option Colonnes à afficher. • Pour ouvrir le fichier CSV dans un paramètre régional différent, utilisez l'option Importer des données de Microsoft Excel. </div>
Colonnes à afficher	Permet de sélectionner ou désélectionner d'autres en-têtes de colonne à répertorier dans le volet Afficher les résultats .
Éléments affichés par page	<p>Permet de spécifier le nombre maximal de journaux à afficher par page. Les options sont les suivantes :</p> <ul style="list-style-type: none"> • 10 • 20 • 50 • 100

3 Cliquez sur **Rechercher**.



Le nombre maximum d'enregistrements pouvant être stockés dans le journal du produit dépend de la taille du fichier journal.

La liste des événements correspondant à vos critères de recherche s'affiche dans la section **Afficher les résultats**.


Importation et exportation de paramètres de configuration

Configurez les paramètres pour exporter la configuration existante du produit (paramètres et stratégies compris) en vue de l'importer et de l'utiliser sur un autre serveur McAfee Security for Microsoft SharePoint. Importez également des listes Sitelist qui spécifient l'emplacement à partir duquel les mises à jour automatiques sont téléchargées.

A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Importer et exporter la configuration**. La page **Importer et exporter des configurations** contient les onglets suivants :

- **Configuration** : permet d'exporter, d'importer ou de restaurer les paramètres du produit.

Tableau 6-10 Onglet Configuration – Définition des options

Option	Définition
Exporter	Permet de copier la configuration du logiciel (paramètres et stratégies) de ce serveur et de l'enregistrer à un emplacement où elle peut être importée par d'autres serveurs McAfee Security for Microsoft SharePoint. Le fichier de configuration du logiciel par défaut s'intitule <code>McAfeeConfigXML.cfg</code> .
Restaurer les valeurs par défaut	Permet de restaurer les paramètres afin de rétablir les performances maximales du produit. Si vous avez personnalisé le produit, le fait de restaurer les valeurs par défaut permet de rétablir les valeurs par défaut de tous les paramètres.
Parcourir	Permet de localiser le fichier de configuration (<code>McAfeeConfigXML.cfg</code>) à importer.
Importer	Permet d'appliquer à ce serveur les paramètres d'un autre serveur McAfee Security for Microsoft SharePoint. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <ul style="list-style-type: none"> • Vous devez importer les paramètres en utilisant la même version du produit sur les deux systèmes. Par exemple, vous ne pouvez pas importer les paramètres d'un serveur McAfee Security for Microsoft SharePoint 2.5 vers un serveur du produit 3.0. • Si vous importez des configurations à partir d'une batterie différente, vous devez alors reconfigurer les tâches d'analyse à la demande. </div>


- **Liste de sites** : permet d'importer des listes Sitelist qui spécifient l'emplacement à partir duquel les mises à jour automatiques sont téléchargées.

Tableau 6-11 Onglet Liste de sites – Définition des options

Option	Définition
Parcourir	Permet de localiser le fichier Sitelist (<code>SiteList.xml</code>) à utiliser.
Importer	Permet d'appliquer les paramètres de configuration de liste de sites spécifiés dans le fichier afin de télécharger les mises à jour des fichiers DAT.

Importation d'une configuration du produit à partir d'un autre serveur

Appliquez à ce serveur les paramètres de configuration du produit d'un autre serveur.

- 

Vous devez importer les paramètres en utilisant la même version du produit sur les deux systèmes. Par exemple, vous ne pouvez pas importer les paramètres d'un serveur McAfee Security for Microsoft SharePoint 2.5 vers un serveur du produit 3.0.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Importer et exporter la configuration**.
La page **Importer et exporter des configurations** s'affiche.
- 2 Cliquez sur l'onglet **Configuration**.
- 3 Dans la section **Importer une configuration**, cliquez sur **Parcourir** pour localiser le fichier de configuration. Le nom du fichier de configuration par défaut est `McAfeeConfigXML.cfg`.

4 Cliquez sur **Importer**.

Une boîte de dialogue affiche le message **Opération terminée avec succès**.

5 Cliquez sur **OK**.

Vous avez à présent terminé l'importation des paramètres de configuration d'un autre serveur du produit vers ce serveur.

Exportation de votre configuration du produit

Exportez la configuration d'un serveur du produit et enregistrez-la à un emplacement où elle peut être importée par d'autres serveurs McAfee Security for Microsoft SharePoint.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Importer et exporter la configuration**.

La page **Importer et exporter des configurations** s'affiche.

2 Cliquez sur l'onglet **Configuration**.**3** Cliquez sur **Exporter**.**4** Spécifiez l'emplacement d'enregistrement du fichier de configuration. Le nom du fichier de configuration par défaut est `McAfeeConfigXML.cfg`.**5** Cliquez sur **Enregistrer**.

Vous avez à présent terminé l'exportation de vos paramètres et stratégies du produit dans un fichier de configuration où ils peuvent être importés par d'autres serveurs McAfee Security for Microsoft SharePoint.

Importation d'une liste Sitelist

Importez une liste Sitelist qui spécifie l'emplacement à partir duquel les mises à jour automatiques sont téléchargées.

Un fichier Sitelist spécifie l'emplacement à partir duquel les mises à jour automatiques sont téléchargées. Par défaut, le logiciel utilise l'**Editeur de liste de sites** qui dirige vers une URL McAfee pour les mises à jour automatiques.

Si le serveur de votre produit est managé par McAfee ePO, les mises à jour automatiques sont effectuées à l'aide de la liste Sitelist ePO. Si vous n'utilisez pas ePO pour manager le serveur de votre produit, créez un fichier Sitelist qui dirigera McAfee Security for Microsoft SharePoint vers un référentiel local.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

1 Cliquez sur **Paramètres et diagnostics | Importer et exporter la configuration**. La page **Importer et exporter des configurations** s'affiche.**2** Cliquez sur l'onglet **Liste de sites**.

- 3 Dans la section **Importer une liste Sitelist**, cliquez sur **Parcourir** pour localiser le fichier Sitelist `SiteList.xml`. Ce fichier contient des informations sur les paramètres de référentiel (nom du référentiel, URL du serveur, etc.).



Vous trouverez le fichier `SiteList.xml` sous le répertoire `C:\ProgramData\McAfee\Common Framework\`. L'application **Editeur de liste de sites** sous **Démarrer | Tous les programmes | McAfee | McAfee Security for Microsoft SharePoint** utilise ce fichier pour afficher les paramètres de référentiel dans l'application.

- 4 Cliquez sur **Importer**.

Une boîte de dialogue affiche le message **Opération terminée avec succès**.

- 5 Cliquez sur **OK**.

Vous avez à présent terminé l'importation de la liste Sitelist pointant vers un nouvel emplacement de référentiel en vue de télécharger des mises à jour de produit.

Configuration des paramètres de fichiers DAT

Vous avez la possibilité de spécifier le nombre d'anciens fichiers DAT pouvant être conservés dans votre système.

Les fichiers DAT sont des fichiers de signatures de détection, également connus sous le nom de fichiers de définitions de détection, qui permettent d'identifier le code que les logiciels antivirus et/ou les programme anti-espion (antispyware) détectent pour remédier aux virus, chevaux de Troie et programmes potentiellement indésirables. Pour obtenir des informations sur le glossaire relatif aux fichiers .DAT, rendez-vous à l'adresse : <http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat>.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Paramètres de DAT**.

La page **Paramètres de DAT** s'affiche.

- 2 Utilisez **Nombre maximal de fichiers DAT obsolètes** pour spécifier le nombre maximal de générations de fichiers DAT à conserver sur le système lors des mises à jour régulières, à l'exclusion du fichier DAT fourni avec la version du produit.



Le logiciel conserve les fichiers DAT les plus récents avec les anciens dans le répertoire `<Dossier d'installation>\bin\DATs`.

- 3 Lors de chaque nouvelle mise à jour de fichiers DAT, le logiciel vérifie le nombre de fichiers DAT disponibles. Si ce nombre dépasse la valeur de conservation de fichiers DAT définie, le plus ancien fichier DAT est supprimé. Vous pouvez indiquer une valeur comprise entre 3 et 10, la valeur par défaut étant 10.
- 4 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration des paramètres utilisateur

Configurez ici les paramètres de l'analyse à l'accès. Quand utilisateur charge ou télécharge des fichiers, l'analyse à l'accès est déclenchée et le logiciel recherche les détections.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres utilisateur**.

La page **Paramètres utilisateur** s'affiche.

- 2 Dans **Paramètres à l'accès**, vous pouvez sélectionner les options suivantes :

Tableau 6-12 Définition des options





Option	Définition
Sur échec d'analyse	<p>Indiquez si vous voulez autoriser ou empêcher le chargement des éléments en cas d'échec de l'analyse.</p> <ul style="list-style-type: none"> • Autoriser • Empêcher le chargement <p> Par défaut, l'option Sur échec d'analyse est définie sur Empêcher le chargement. Il n'est pas recommandé de modifier ce paramètre.</p>
Récupérer les paramètres AV de SharePoint toutes les (minutes)	<p>Spécifiez la durée (en minutes) pour récupérer les paramètres antivirus à partir du serveur SharePoint.</p> <p> Nous vous recommandons de spécifier une durée moindre de sorte que le tableau de bord se synchronise avec vos paramètres antivirus SharePoint.</p>
Taille maximale de la zone de quarantaine	<p>Indiquez la taille maximale de l'élément en quarantaine, en Mo ou Ko. Vous pouvez spécifier une valeur comprise entre 1 et 102400 Ko ou 1 et 100 Mo, où la valeur par défaut est 3125 Ko.</p>
Nombre maximum d'analyseurs	<p>Spécifiez le nombre maximal de comptes d'analyseur. Vous pouvez indiquer une valeur comprise entre 1 et 5. La valeur par défaut est 5.</p> <p>Le compte d'analyseur spécifie le nombre de threads à la fois que le logiciel accepte pour le traitement.</p>
Ajouter des pools d'applications à recycler	<p>Spécifiez un pool d'applications que vous voulez ajouter au produit.</p> <p>Les pools d'applications servent à séparer des processus distincts qui partagent la même configuration ou les mêmes limites d'applications. Ils sont utilisés pour isoler des applications web pour plus de sécurité, de fiabilité et de performances. Une fois installé, McAfee Security for Microsoft SharePoint crée un pool d'applications <i>MSMSAppPool</i> de façon à ne pas affecter le serveur SharePoint. Si vous avez des pools d'applications personnalisés pour votre organisation et que vous voulez les ajouter au serveur du produit, vous pouvez les ajouter à l'aide de cette option.</p>
Ajouter un pool d'applications	<p>Spécifiez un pool d'applications dans Ajouter des pools d'applications à recycler, puis cliquez Ajouter.</p> <p> Ajoutez tous les pools d'applications où des sites SharePoint s'exécutent.</p>

Tableau 6-12 Définition des options

Option	Définition
Pools d'applications existants à recycler :	Affiche la liste des pools d'applications configurés pour ce serveur SharePoint.
Supprimer un pool d'applications	<p>Sélectionnez un pool d'applications dans Pools d'applications existants à recycler : et cliquez sur Supprimer pour exclure les pools d'applications qui ne sont plus nécessaires.</p> <div data-bbox="634 457 1523 527" style="background-color: #f0f0f0; padding: 5px;"> <p> Pour sélectionner plusieurs pools d'applications, utilisez les commandes Ctrl+clic ou Maj+clic.</p> </div>

3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Vous avez à présent terminé la configuration des paramètres à l'accès de votre produit.

7

Maintenance du programme

Procédez à des tâches de maintenance telles que la réparation, la purge ou la suppression de McAfee Security for Microsoft SharePoint.

Sommaire

- ▶ *Réparation de l'installation*
- ▶ *Purge et optimisation*
- ▶ *Restauration de la configuration par défaut*
- ▶ *Désinstallation du logiciel*

Réparation de l'installation

Vous pouvez résoudre les erreurs d'installation dans le programme en corrigeant les fichiers, les raccourcis et les entrées de Registre manquants ou corrompus.



Vous pouvez également réparer l'installation à partir du dossier contenant les fichiers d'installation, en cliquant sur `setup.exe`. La réparation d'une installation rétablit les paramètres de configuration par défaut.

Procédure

- 1 Cliquez sur **Démarrer** | **Paramètres** | **Panneau de configuration**.
- 2 Double-cliquez sur **Ajout/Suppression de programmes**. La fenêtre **Ajout/Suppression de programmes** apparaît.
- 3 Cliquez sur **McAfee Security for Microsoft SharePoint** dans la liste, puis sur **Modifier**. L'assistant d'installation s'affiche, suivi de la boîte de dialogue **Maintenance de l'application**, avec l'option **Réparer** sélectionnée par défaut.
- 4 Cliquez sur **Suivant**. La boîte de dialogue **Compte de la base de données** s'affiche.
- 5 Modifiez comme demandé les **informations du compte**.



Si les références d'identification d'utilisateur ne peuvent être résolues par le serveur, une boîte de dialogue d'avertissement vous invite à vérifier vos références d'identification.

- 6 Vérifiez si vous avez saisi les références d'identification correctes. Cliquez sur **OK**, puis sur **Suivant** pour ignorer l'avertissement et poursuivre la procédure de réparation avec des informations de compte non résolues.



La réparation de l'installation rétablit la version des fichiers DAT et de moteur installés à l'origine par le produit. Il est recommandé de procéder à une mise à jour une fois l'installation terminée.

La boîte de dialogue **Prêt à réparer l'application** s'affiche.

- 7 Cliquez sur **Suivant**. La fenêtre **Mise à jour du système** s'affiche. Une fois McAfee Security for Microsoft SharePoint mis à jour, un message de confirmation s'affiche.
- 8 Sélectionnez ou désélectionnez les options suivantes selon vos besoins, puis cliquez sur **Terminer**.
 - **Lancer l'interface utilisateur** : pour lancer l'interface utilisateur graphique du produit.
 - **Mettre à jour** : pour télécharger les dernières mises à jour du produit et vous assurer ainsi d'appliquer les mesures de sécurité les plus actuelles pour lutter contre des menaces en constante évolution.

Purge et optimisation

Supprimez de la base de données les anciens éléments marqués pour la suppression et effectuez la tâche d'optimisation afin de récupérer l'espace disque occupé par les enregistrements de base de données supprimés.

Procédure

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Éléments détectés**.

La page **Éléments détectés** s'affiche.

- 2 A partir de la section **Base de données locale**, vous pouvez utiliser les options suivantes :
 - **Fréquence de purge des éléments anciens** : permet de spécifier la périodicité à laquelle les anciens éléments marqués pour la suppression sont effectivement supprimés de la base de données. La valeur par défaut est **Quotidienne**.
 - **Fréquence d'optimisation** : permet de récupérer l'espace disque occupé par les enregistrements de base de données supprimés. En fonction de la valeur définie sous **Age maximal de l'élément (jours)**, les anciens enregistrements seront supprimés si vous avez planifié une tâche de purge. Afin d'optimiser la base de données, planifiez une tâche d'optimisation.



Pensez à toujours planifier une tâche d'optimisation quelques heures après avoir effectué une tâche de purge.

- 3 Cliquez sur **Modifier le calendrier** pour modifier le calendrier. Vous pouvez choisir un horaire en fonction des options.
 - **Non planifiée** : sélectionnez cette option si vous n'avez pas décidé du moment où vous souhaitez exécuter la tâche de purge ou d'optimisation.
 - **Une fois** : spécifiez les date et heure auxquelles vous souhaitez planifier une tâche unique de purge ou d'optimisation.
 - **Heures** : sélectionnez cette option pour planifier la tâche de purge ou d'optimisation selon le nombre d'heures spécifié.
 - **Jours** : sélectionnez cette option pour planifier la tâche de purge ou d'optimisation en fonction du nombre d'exécutions hebdomadaires souhaité.
 - **Semaines** : sélectionnez cette option pour planifier la tâche de purge ou d'optimisation en fonction du nombre d'exécutions mensuelles souhaité.
 - **Mois** : sélectionnez cette option pour planifier la tâche de purge ou d'optimisation en fonction du nombre d'exécutions annuelles souhaité.



Ces tâches doivent être effectuées régulièrement pour libérer de l'espace dans la base de données.

Restauration de la configuration par défaut

Restaurez la configuration par défaut du produit.

Procédure

- 1 A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics | Importer et exporter la configuration**. La page **Importer et exporter des configurations** s'affiche.
- 2 Sous l'onglet **Configuration**, cliquez sur **Restaurer les paramètres par défaut**.



La restauration des paramètres par défaut entraîne la suppression de tous les paramètres de stratégie et sous-stratégies configurés. Il est conseillé d'effectuer une sauvegarde des paramètres existants à des fins de restauration ultérieure.

Une boîte de dialogue s'affiche, vous invitant à confirmer les paramètres.

- 3 Cliquez sur **OK**.

Une boîte de dialogue s'affiche, confirmant l'application des paramètres de configuration par défaut.

Vous avez à présent terminé la restauration des paramètres de configuration par défaut du serveur McAfee Security for Microsoft SharePoint en vue d'optimiser les performances.

Désinstallation du logiciel

Supprimez ou désinstallez le logiciel installé sur le serveur.



Vous pouvez également supprimer le logiciel à partir du dossier contenant les fichiers d'installation en double-cliquant sur `setup.exe`.

Procédure

- 1 Cliquez sur **Démarrer | Paramètres | Panneau de configuration**.
- 2 Double-cliquez sur **Ajout/Suppression de programmes**. La fenêtre **Ajout/Suppression de programmes** apparaît.
- 3 Cliquez sur **McAfee Security for Microsoft SharePoint** dans la liste, puis sur **Désinstaller**.



Une alternative consiste à double-cliquer sur **McAfee Security for Microsoft SharePoint** dans la liste.

- 4 Cliquez sur **Oui**. Une barre de progression s'affiche pour indiquer le statut de la procédure. Une fois la désinstallation terminée, le nom du produit est supprimé de la liste **Ajout/Suppression de programmes**.

8

Intégration avec ePolicy Orchestrator

Vous pouvez intégrer et gérer le produit à l'aide du logiciel de gestion ePolicy Orchestrator.

McAfee ePO est une plate-forme évolutive destinée à la gestion et à la mise en œuvre centralisées de stratégies pour vos produits de sécurité McAfee et les systèmes sur lesquels ils sont installés. Elle propose également des fonctionnalités complètes de déploiement de produits et de génération de rapports, par l'intermédiaire d'un point de contrôle unique.

Vous pouvez intégrer ce produit avec McAfee ePO 4.5, 4.6 et 5.0.

Pour obtenir des instructions concernant la configuration et l'utilisation de McAfee ePO, consultez le Guide Produit correspondant à votre version.

Sommaire

- ▶ *Configuration système requise*
- ▶ *Archivage du package logiciel*
- ▶ *Installation des extensions logicielles*
- ▶ *Migration de stratégies à partir d'une ancienne version*
- ▶ *Déploiement du logiciel sur les clients*
- ▶ *Gestion des stratégies*
- ▶ *Création et planification de tâches*
- ▶ *Requêtes et rapports*
- ▶ *Filtrage des événements*
- ▶ *Suppression du logiciel*

Configuration système requise

Configurez votre environnement avant d'intégrer le produit avec ePolicy Orchestrator.

- Utilisez les informations d'identification d'administrateur du serveur ePolicy Orchestrator.
- Ajoutez des nœuds gérables au serveur ePolicy Orchestrator sur lequel vous voulez déployer McAfee Security for Microsoft SharePoint. Consultez la documentation produit ePolicy Orchestrator pour des instructions.
- Déployez McAfee Agent sur vos nœuds gérés exécutant Microsoft SharePoint. Consultez la documentation produit McAfee Agent pour les instructions d'installation.
- Si vous effectuez une mise à niveau depuis une version précédente, désinstallez toutes les éventuelles versions antérieures du produit autres que McAfee Security for Microsoft SharePoint 2.5 Correctif 1.
- Assurez-vous de disposer des informations d'identification d'administrateur pour chaque serveur SharePoint en mode serveur unique ou environnement batterie.
- Choisissez le port ouvert/non utilisé sur le serveur où vous voulez héberger le site McAfee Security for Microsoft SharePoint.

Archivage du package logiciel

Archivez le package de déploiement de McAfee Security for Microsoft SharePoint sur le serveur ePolicy Orchestrator.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Logiciels | Référentiel maître**, puis sur **Action | Archiver un package**.
- 3 A l'étape **Package**, sélectionnez **Produit ou mise à jour (.ZIP)**, cliquez sur **Parcourir**, accédez au fichier .zip contenant le package logiciel, puis cliquez sur **Suivant**.
- 4 A l'étape **Options du package**, sélectionnez **Actuels** comme branche, puis cliquez sur **Enregistrer**.

Installation des extensions logicielles

Installez les extensions logicielles sur le serveur ePolicy Orchestrator.



Même si une précédente version de l'extension logicielle est installée, cette tâche ajoute l'extension McAfee Security for Microsoft SharePoint 3.0 à la liste. Vous pouvez conserver les précédentes extensions ou les supprimer, selon le cas.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Choisissez **Menu | Logiciels | Extensions**, puis cliquez sur **Installer une extension**.
- 3 Cliquez sur **Parcourir**, accédez au fichier .zip contenant l'extension (`MSMS30PolicyEx_0409.zip` pour le français), puis cliquez sur **OK**.



Installez l'extension de rapport, puis l'extension de l'aide de la même manière.

Migration de stratégies à partir d'une ancienne version

Lors de la mise à niveau du logiciel, vous avez la possibilité de migrer les stratégies existantes à partir d'anciennes versions vers McAfee Security for Microsoft SharePoint 3.0.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Parcourez l'arborescence du système jusqu'au dossier contenant le fichier `MSMS_ePOUpgrade.zip`, puis extrayez ce dernier.



Assurez-vous que tous les fichiers contenus dans le .zip sont extraits vers le même dossier.

- 2 A partir de l'invite de commande, accédez au dossier contenant le fichier .zip extrait, puis exécutez la commande `MSMSePOUpgrade.exe`.

- 3 Saisissez le mot de passe de la base de données ePolicy Orchestrator, puis appuyez sur **Entrée**.
- 4 Saisissez le nom de l'instance SQL de ePolicy Orchestrator si vous avez créée une telle instance au cours de l'installation du serveur, sinon ne renseignez pas ce champ. Appuyez ensuite sur **Entrée**.

La mise à niveau des stratégies commence. Patientez jusqu'à son terme.

Une fois le processus terminé, un message de confirmation s'affiche. Pour des détails sur les informations consignées, consultez le fichier `EPODebugTrace.txt` dans le répertoire actif. Appuyez sur **Entrée** pour quitter le processus.

- Vérifiez que les stratégies ont effectivement été mises à niveau : Dans la console ePolicy Orchestrator, accédez au **Catalogue de stratégies**, sélectionnez le produit **McAfee Security for Microsoft SharePoint 3.0.0**, puis repérez les stratégies mises à niveau signalées par le suffixe (**Upgraded**) (Mis à niveau). Exemple : **My Default (Upgraded)**.
- Affectez les stratégies personnalisées aux systèmes nécessaires, sans quoi les stratégies McAfee par défaut seront mises en œuvre.

Déploiement du logiciel sur les clients

Déployez le logiciel sur les systèmes clients Microsoft SharePoint.

Avant de commencer

Migrez les stratégies existantes à partir d'anciennes versions vers McAfee Security for Microsoft SharePoint 3.0.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.



Lors de la mise à niveau du logiciel, veillez à sélectionner tous les systèmes nécessaires.

- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Agent .
3 Sélectionnez Déploiement de produit comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Déploiement de produit .
4 Sélectionnez Windows comme plate-forme cible.	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et des remarques le cas échéant.
	6 Sélectionnez Windows comme plate-forme cible.

- 4 Sous **Produits et composants**, sélectionnez **McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxx**, choisissez **Installer** comme action, sélectionnez la langue, puis cliquez sur **Enregistrer**.



Tapez les références d'identification du système où est installé le serveur SharePoint dans la ligne de commande d'ePolicy Orchestrator.

- REMOTESQLUSER = "NomDomaine\NomUtilisateur ou NomHôte\NomUtilisateur"
- REMOTESQLPWD = "motdepasse"
- IISPORT = 45900 (Facultatif)

- 5 Planifiez la tâche pour une exécution immédiate, puis cliquez sur **Suivant** afin d'afficher une synthèse de la tâche.
- 6 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.
- 7 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 8 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Une fois la tâche exécutée correctement, le logiciel est déployé sur les systèmes sélectionnés.

Gestion des stratégies

Les stratégies de McAfee Security for Microsoft SharePoint fournissent des options permettant la configuration des stratégies, ainsi que l'activation, la désactivation, la configuration et l'administration des fonctionnalités et des journaux associés.

Ces paramètres de stratégie sont très semblables à ceux qui sont accessibles sous l'onglet **Gestionnaire de stratégies** et **Paramètres et diagnostics** de l'interface utilisateur du produit.

Ces stratégies sont disponibles via la page **Catalogue de stratégies** sous le produit **McAfee Security for Microsoft SharePoint**.

- **Paramètres de l'analyseur** : permet de modifier les paramètres pour les stratégies à l'accès ou à la demande.
- **Paramètres et diagnostics** : permet de modifier les paramètres liés à l'activation, la désactivation, la configuration et l'administration des fonctionnalités et des journaux associés.

Modifiez les stratégies en fonction de vos préférences, puis affectez-les à des groupes de systèmes Microsoft SharePoint managés ou à un seul système. Pour des informations d'ordre général concernant les stratégies, consultez le Guide Produit de votre version du logiciel ePolicy Orchestrator.

Procédures

- [Créer ou modifier des stratégies, page 101](#)
Créer ou modifier des stratégies McAfee Security for Microsoft SharePoint à partir de la page **Catalogue de stratégies**.
- [Affectation de stratégies, page 101](#)
Une fois que vous avez créé ou modifié les stratégies de produit à l'aide des paramètres appropriés, affectez chacune d'elles aux systèmes Microsoft SharePoint requis qui sont gérés par ePolicy Orchestrator.

Créez ou modifiez des stratégies

Créez ou modifiez des stratégies McAfee Security for Microsoft SharePoint à partir de la page **Catalogue de stratégies**.

Une autre solution consiste à créer ou à modifier ces stratégies à partir de l'**Arborescence des systèmes** tout en affectant des stratégies aux systèmes sélectionnés. Pour plus d'informations à ce sujet, consultez le Guide Produit de votre version du logiciel ePolicy Orchestrator.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 A partir de la page **Catalogue de stratégies**, sélectionnez **McAfee Security for Microsoft SharePoint 3.0.0** comme produit, puis sélectionnez la stratégie requise comme catégorie.
- 3 Effectuez cette étape en fonction de vos besoins :

Pour créer une stratégie	Pour modifier une stratégie
Cliquez sur Nouvelle stratégie , saisissez un nom pour la stratégie, puis cliquez sur OK .	Cliquez sur la stratégie à modifier.

- 4 Modifiez les paramètres de stratégie le cas échéant, puis cliquez sur **Enregistrer**.

Les paramètres de stratégie sont mis à jour et la nouvelle stratégie (en cas de création) figure dans le **Catalogue de stratégies**.

Affectation de stratégies

Une fois que vous avez créé ou modifié les stratégies de produit à l'aide des paramètres appropriés, affectez chacune d'elles aux systèmes Microsoft SharePoint requis qui sont gérés par ePolicy Orchestrator.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Accédez à **Arborescence des systèmes**, sélectionnez le groupe ou les systèmes requis, puis cliquez sur l'onglet **Stratégies affectées**.
- 3 Sélectionnez **McAfee Security for Microsoft SharePoint 3.0.0** dans la liste des produits, localisez la stratégie appropriée, puis cliquez sur **Modifier l'affectation** en regard de la stratégie.
- 4 (Facultatif) Sélectionnez une stratégie, puis cliquez sur **Modifier la stratégie** pour modifier les paramètres de la stratégie. Cliquez sur **Nouvelle stratégie** pour créer une stratégie basée sur la catégorie sélectionnée.



Une autre solution consiste à modifier ou à créer une stratégie à partir de la page **Catalogue de stratégies**.

- 5 Sélectionnez la stratégie à affecter, configurez les options d'héritage appropriées, puis cliquez sur **Enregistrer**.

La mise en œuvre de la stratégie se produit lors de la prochaine communication agent-serveur. Cliquez sur **Réactiver les agents** afin de mettre en œuvre immédiatement les stratégies.

Création et planification de tâches

Créez des tâches client sur les systèmes Microsoft SharePoint en vue de planifier des actions automatisées.

Procédures

- [Planification de mises à jour automatiques, page 102](#)
Planifiez des mises à jour automatiques afin de maintenir votre logiciel à jour avec la dernière version des définitions antivirus (fichiers DAT) et du moteur d'analyse antivirus.
- [Planification d'une analyse à la demande, page 103](#)
Planifiez une analyse à la demande de vos serveurs Microsoft SharePoint afin de détecter d'éventuelles menaces, vulnérabilités ou autre code potentiellement indésirable.
- [Planification d'une tâche d'optimisation, page 103](#)
Planifiez une tâche d'optimisation afin de récupérer l'espace disque occupé par les enregistrements de base de données supprimés.
- [Planification d'une tâche de purge des anciens fichiers DAT, page 104](#)
Planifiez une tâche de purge des anciens fichiers DAT pour les supprimer.
- [Planification d'une tâche de purge, page 105](#)
Planifiez une tâche de purge pour supprimer les anciens éléments de la base de données.

Planification de mises à jour automatiques

Planifiez des mises à jour automatiques afin de maintenir votre logiciel à jour avec la dernière version des définitions antivirus (fichiers DAT) et du moteur d'analyse antivirus.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et Version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Security for Microsoft SharePoint 3.0.0 .
3 Sélectionnez Tâche AutoUpdate (Mise à jour automatique) (McAfee Security for Microsoft SharePoint 3.0.0) comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Tâche AutoUpdate (Mise à jour automatique) .
4 Aucune configuration n'étant nécessaire à l'étape 2, cliquez à nouveau sur Suivant .	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et une description, puis cliquez ensuite sur Enregistrer . La tâche est répertoriée sous Nom de la tâche .
	6 Sélectionnez la tâche, puis cliquez sur Suivant .

- 4 Planifiez la tâche selon vos besoins, puis cliquez sur **Suivant** pour afficher une synthèse de la tâche.
- 5 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.

- 6 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 7 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Planification d'une analyse à la demande

Planifiez une analyse à la demande de vos serveurs Microsoft SharePoint afin de détecter d'éventuelles menaces, vulnérabilités ou autre code potentiellement indésirable.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et Version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Security for Microsoft SharePoint 3.0.0 .
3 Sélectionnez Tâche d'analyse à la demande (McAfee Security for Microsoft SharePoint 3.0.0) comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Analyse à la demande .
	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et une description.

- 4 Dans **Choisir les éléments à analyser**, tapez le nom d'application web et le chemin d'accès au dossier cible, puis cliquez sur >> pour déplacer le(s) dossier(s) vers les dossiers à analyser.

Exemple :

Nom d'application web — SharePoint - 80

Chemin d'accès au dossier cible — http://nomhôte/valeurdéfaut/nomdossier

- 5 Sélectionnez les dossiers à analyser et configurez les paramètres de l'analyse en spécifiant les éventuelles extensions de fichier à exclure et l'analyse avec reprise ou incrémentielle.
- 6 Planifiez la tâche selon vos besoins, puis cliquez sur **Suivant** et sur **Enregistrer**.
- 7 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 8 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Planification d'une tâche d'optimisation

Planifiez une tâche d'optimisation afin de récupérer l'espace disque occupé par les enregistrements de base de données supprimés.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et Version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Security for Microsoft SharePoint 3.0.0 .
3 Sélectionnez Tâche d'optimisation (McAfee Security for Microsoft SharePoint 3.0.0) comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Tâche d'optimisation .
4 Aucune configuration n'étant nécessaire à l'étape 2, cliquez à nouveau sur Suivant .	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et une description, puis cliquez ensuite sur Enregistrer . La tâche est répertoriée sous Nom de la tâche .
	6 Sélectionnez la tâche, puis cliquez sur Suivant .

- 4 Planifiez la tâche selon vos besoins, puis cliquez sur **Suivant** pour afficher une synthèse de la tâche.
- 5 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.
- 6 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 7 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Planification d'une tâche de purge des anciens fichiers DAT

Planifiez une tâche de purge des anciens fichiers DAT pour les supprimer.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et Version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Security for Microsoft SharePoint 3.0.0 .
3 Sélectionnez Tâche PurgeOldDATs (Purge des anciens fichiers DAT) (McAfee Security for Microsoft SharePoint 3.0.0) comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Tâche PurgeOldDATs (Purge des anciens fichiers DAT) .
4 Aucune configuration n'étant nécessaire à l'étape 2, cliquez à nouveau sur Suivant .	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et une description.
	6 La tâche est répertoriée sous Nom de la tâche .
	7 Sélectionnez la tâche, puis cliquez sur Suivant .

- 4 Planifiez la tâche selon vos besoins, puis cliquez sur **Suivant** pour afficher une synthèse de la tâche.
- 5 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.
- 6 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 7 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Planification d'une tâche de purge

Planifiez une tâche de purge pour supprimer les anciens éléments de la base de données.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6 et version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Security for Microsoft SharePoint 3.0.0 .
3 Sélectionnez Tâche de purge (McAfee Security for Microsoft SharePoint 3.0.0) comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Tâche de purge .
4 Aucune configuration n'étant nécessaire à l'étape 2, cliquez à nouveau sur Suivant .	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
	5 Saisissez un nom pour la tâche et une description.
	6 La tâche est répertoriée sous Nom de la tâche .
	7 Sélectionnez la tâche, puis cliquez sur Suivant .

- 4 Planifiez la tâche selon vos besoins, puis cliquez sur **Suivant** pour afficher une synthèse de la tâche.
- 5 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.
- 6 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 7 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Requêtes et rapports

Exécutez les requêtes McAfee Security for Microsoft SharePoint prédéfinies en vue de générer des rapports ou modifiez-les afin de produire des rapports personnalisés.

Requêtes prédéfinies

Ces requêtes prédéfinies sont ajoutées au groupe **McAfee Security for Microsoft SharePoint Reports** dans ePolicy Orchestrator 4.6 et au groupe **MSMS30REPORTS** dans ePolicy Orchestrator 4.5. et 5.0.

Requête	Informations récupérées
MSMS : historique de conformité et DLP	Données historiques relatives à la catégorie de menaces Conformité et DLP de tous les serveurs managés du produit.
MSMS : historique des messages/types de fichiers interdits	Données historiques relatives à la catégorie de menaces des types de fichiers et des messages interdits de tous les serveurs managés du produit.
MSMS : messages/types de fichiers interdits aujourd'hui	Le nombre de types de fichiers et de messages interdits du jour.
MSMS : Nombre de documents et durée moyenne de traitement aujourd'hui	Nombre de documents analysés sur chaque serveur managé du produit ce jour et durée moyenne de l'analyse.
MSMS : pourcentage de programmes potentiellement indésirables détectés aujourd'hui	Pourcentage de programmes potentiellement indésirables ayant infecté des éléments qui ont été détectés sur chaque serveur ce jour.
MSMS : pourcentage de virus détectés aujourd'hui	Pourcentage de virus ayant infecté des éléments qui ont été détectés sur chaque serveur ce jour.

Requête	Informations récupérées
MSMS : programmes potentiellement indésirables supprimés aujourd'hui	Les documents infectés par des programmes potentiellement indésirables supprimés ce jour.
MSMS : historique des détections de programmes potentiellement indésirables	Récapitulatif des programmes potentiellement indésirables ayant infecté des documents qui ont été détectés.
MSMS : détection de programmes potentiellement indésirables aujourd'hui	Les documents infectés par des programmes potentiellement indésirables détectés ce jour.
MSMS : 10 principaux messages/types de fichiers interdits	10 principaux types de fichier/messages interdits par le nombre de détections.
MSMS : 10 principaux expéditeurs d'événements de conformité et DLP	10 principaux expéditeurs d'événements de conformité et DLP par le nombre de détections.
MSMS : 10 principaux serveurs SharePoint infectés	10 principaux serveurs SharePoint par le nombre d'éléments infectés détectés.
MSMS : 10 principaux emplacements avec chargements d'événements de conformité et DLP	10 principaux emplacements de serveurs SharePoint qui ont des problèmes de chargement de conformité et DLP.
MSMS : 10 principaux chargements de contenu indésirable	10 principaux contenus potentiellement indésirables par leur nombre de détections.
MSMS : 10 principaux emplacements avec chargements de virus	10 principaux emplacements de serveurs SharePoint qui affichent le maximum de chargements de virus.
MSMS : 10 principales détections de programmes potentiellement indésirables	10 principaux contenus potentiellement indésirables détectés par leurs emplacements de serveurs.
MSMS : 10 premières détections de contenu indésirable	10 principaux contenus indésirables détectés dans les éléments.
MSMS : 10 principaux expéditeurs de contenu indésirable	10 principaux serveurs SharePoint comportant un contenu indésirable.
MSMS : 10 principaux expéditeurs de virus	10 principaux serveurs SharePoint qui ont le nombre maximum de documents infectés par des virus.
MSMS : 10 principales détections de virus	10 principaux documents ou éléments qui ont le maximum de virus.
MSMS : historique des détections de virus	Nombre de virus ayant infecté des éléments qui ont été détectés.
MSMS : détections de virus aujourd'hui	Nombre d'éléments infectés par des virus détectés ce jour.
MSMS : Virus nettoyés/remplacés aujourd'hui	Nombre d'éléments infectés par des virus nettoyés ce jour.
MSMS : virus détectés au cours de la dernière semaine	Nombre d'éléments infectés par des virus détectés la semaine dernière.

Exécution d'une requête par défaut

Exécutez les requêtes McAfee Security for Microsoft SharePoint prédéfinies pour générer des rapports basés sur des données du produit.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous à ePolicy Orchestrator en tant qu'administrateur.
- 2 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator :

Version 4.5	Version 4.6	Version 5.0
1 Cliquez sur Menu Rapports Requêtes .	1 Cliquez sur Menu Rapports Requêtes et rapports .	1 Cliquez sur Menu Requêtes et rapports .
2 Dans le volet Groupes , sous Groupes partagés , sélectionnez MSMS30REPORTS .	2 Dans le volet Groupes , sous Groupes partagés , sélectionnez McAfee Security for Microsoft SharePoint Reports .	2 Dans le volet Groupes , sous Groupes partagés , sélectionnez MSMS30REPORTS .

- 3 Sélectionnez une requête dans la liste **Requêtes**, puis cliquez sur **Exécuter**. Dans la page des résultats de la requête, cliquez sur l'un des résultats pour accéder aux détails sous-jacents.



Pour générer des rapports personnalisés, dupliquez une requête prédéfinie, puis modifiez-la en fonction de vos exigences. Pour des instructions détaillées sur l'utilisation des requêtes, consultez le Guide Produit correspondant à votre version du logiciel ePolicy Orchestrator.

Filtrage des événements

Spécifiez les événements McAfee Security for Microsoft SharePoint générés à partir des systèmes clients qui sont à transférer au serveur.

Par défaut, tous les événements concernant le produit sont activés. Filtrez les événements en fonction de la bande passante consommée dans votre environnement et des requêtes basées sur les événements nécessaires.

Pour plus de détails sur le filtrage des événements, consultez le Guide Produit de votre version du logiciel ePolicy Orchestrator.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Choisissez **Menu | Configuration | Paramètres serveur**, sélectionnez **Filtrage des événements**, puis cliquez sur **Modifier** au bas de la page.
- 3 Sélectionnez **Tous les événements au serveur** pour transférer tous les événements au serveur ePolicy Orchestrator ou **Uniquement les événements sélectionnés au serveur** et spécifiez les événements clients du produit à transférer.

Les événements concernant le produit sont dotés de préfixes **McAfee Security for Microsoft SharePoint** de ce type :

- 6054 : McAfee Security for Microsoft SharePoint Contenu chiffré détecté (Bas)
- 6055 : McAfee Security for Microsoft SharePoint Contenu corrompu détecté (Bas)
- 6056 : McAfee Security for Microsoft SharePoint Dénier de service déclenché (Moyen)
- 6057 : McAfee Security for Microsoft SharePoint Contenu protégé déclenché (Bas)
- 6058 : McAfee Security for Microsoft SharePoint Contenu protégé par mot de passe détecté (Bas)
- 6059 : McAfee Security for Microsoft SharePoint Type MIME bloqué détecté (Bas)
- 6060 : McAfee Security for Microsoft SharePoint Statistiques MSMS et durée moyenne de l'analyse (Informations)

- 4 Cliquez sur **Enregistrer**.

Les événements sélectionnés sont transférés lors de la prochaine communication agent-serveur.

Suppression du logiciel

Supprimez le logiciel client et les extensions McAfee Security for Microsoft SharePoint pour éliminer le logiciel et ses fonctionnalités.

Pour supprimer entièrement le logiciel et ses fonctionnalités au sein de votre environnement, supprimez les différents composants en respectant l'ordre suivant :

- 1 Supprimez le logiciel client McAfee Security for Microsoft SharePoint installé sur les clients.
- 2 Supprimez les extensions du logiciel McAfee Security for Microsoft SharePoint dans cet ordre.
 - a Extension de rapports.
 - b Extension de stratégie.
 - c Extension d'aide.

Procédures

- [Suppression du logiciel des systèmes clients, page 109](#)
Créez une tâche client destinée à supprimer le logiciel client McAfee Security for Microsoft SharePoint installé sur les serveurs Microsoft SharePoint managés.
- [Suppression des extensions logicielles, page 110](#)
Retirez les extensions du produit du serveur ePolicy Orchestrator.

Suppression du logiciel des systèmes clients

Créez une tâche client destinée à supprimer le logiciel client McAfee Security for Microsoft SharePoint installé sur les serveurs Microsoft SharePoint managés.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Cliquez sur **Menu | Systèmes | Arborescence des systèmes**, puis sélectionnez le groupe ou les systèmes requis.
- 3 Effectuez les étapes suivantes en fonction de votre version d'ePolicy Orchestrator.

Version 4.5	Version 4.6 et Version 5.0
1 Cliquez sur l'onglet Tâches client , puis sur Nouvelle tâche . L'écran Générateur de tâches client s'affiche.	1 Activez l'onglet Tâches client affectées , puis cliquez sur Actions Nouvelle affectation de tâche client . L'écran Générateur d'affectations de tâche client s'affiche.
2 Saisissez un nom pour la tâche et des remarques le cas échéant.	2 Sous Produit , sélectionnez McAfee Agent .
3 Sélectionnez Déploiement de produit comme type de tâche, puis cliquez sur Suivant .	3 Sous Type de tâche , sélectionnez Déploiement de produit .
4 Sélectionnez Windows comme plate-forme cible.	4 Cliquez sur Créer une tâche . L'écran Catalogue de tâches client s'affiche.
5 Sous Produits et composants , sélectionnez McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxx , choisissez Supprimer comme action, sélectionnez la langue, puis cliquez sur Suivant .	5 Saisissez un nom pour la tâche et des remarques le cas échéant.
	6 Sélectionnez Windows comme plate-forme cible.
	7 Sous Produits et composants , sélectionnez McAfee Security for Microsoft SharePoint - xxxxxxxx 3.0.0.xxx , choisissez Supprimer comme action, sélectionnez la langue, puis cliquez sur Enregistrer . La tâche est répertoriée sous Nom de la tâche .
	8 Sélectionnez la tâche, puis cliquez sur Suivant .

- 4 Planifiez la tâche pour une exécution immédiate, puis cliquez sur **Suivant** afin d'afficher une synthèse de la tâche.
- 5 Consultez la synthèse de la tâche, puis cliquez sur **Enregistrer**.
- 6 A la page **Arborescence des systèmes**, sélectionnez les systèmes ou les groupes auxquels la tâche est affectée, puis cliquez sur **Réactiver les agents**.
- 7 Dans l'écran **Réactiver McAfee Agent**, sélectionnez **Forcer la mise à jour complète des stratégies et des tâches**, puis cliquez sur **OK**.

Suppression des extensions logicielles

Retirez les extensions du produit du serveur ePolicy Orchestrator.

Avant de commencer

Si McAfee Security for Microsoft SharePoint signale qu'une extension est installée, supprimez-la avant de supprimer l'extension du produit.

Procédure

Pour consulter la définition des options, cliquez sur ? dans l'interface.

- 1 Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur.
- 2 Pour supprimer l'extension de rapport, cliquez sur **Menu | Logiciel | Extensions**.
- 3 Sélectionnez **McAfee Security for Microsoft SharePoint** dans le volet de gauche.

- 4 Cliquez sur **Supprimer** en regard de l'extension de rapport, sélectionnez **Forcer la suppression en ignorant les recherches et les erreurs**, puis cliquez sur **OK**.
Recommencez cette étape pour supprimer l'extension de stratégie **McAfee Security for Microsoft SharePoint 3.0** (MSMS____3000.ZIP).
- 5 Pour supprimer l'extension de l'aide, sélectionnez **Contenu de l'aide** dans le volet gauche, puis cliquez sur **Supprimer** en regard de **msms_help**.

A

Création d'un compte d'utilisateur de domaine personnalisé avec des autorisations SQL minimales

Si la stratégie de votre organisation vous empêche d'utiliser les informations d'identification d'administrateur ou si vous ne voulez pas les utiliser pour d'autres raisons, vous pouvez créer un compte d'utilisateur de domaine normal personnalisé avec des autorisations SQL minimales.

Active Directory

- 1 Créez un nouveau compte d'utilisateur de domaine dans Active Directory. (Par exemple : MSMSDBAcnt).
- 2 Affectez au compte des privilèges équivalents à ceux des membres du groupe Utilisateurs.
- 3 Le programme d'installation du produit vous invite à saisir les identifiants du compte lors de la configuration du compte d'accès de base de données pour une connexion SQL à distance.

SQL Server

- 1 Des droits d'administrateur SQL Server sont requis pour effectuer des mises à jour de groupe. Apportez ces modifications sous la sécurité de SQL Server :
 - a Ajoutez le compte d'utilisateur personnalisé (par exemple : MSMSDBAcnt) à utiliser pour le compte d'accès de la base de données de McAfee Security for Microsoft SharePoint. Fournissez les autorisations publiques à l'utilisateur.
 - b Sous le mappage d'utilisateurs, sélectionnez :
 - Toutes les bases de données de contenu SharePoint correspondant à des applications Web.
 - La base de données de contenu correspondant à votre application Web d'administrateur.
 - La base de données de configuration SharePoint.
- 2 Accordez ces autorisations.
 - Affectez aux éléments sécurisables ci-dessous les droits d'exécution pour la base de données de configuration SharePoint (la liste exacte peut être légèrement différente)

Éléments sécurisables	
proc_getObjectsByBaseClass	proc_getSiteMap
proc_getSiteSubset	proc_getObjectsByClass
proc_getSiteMapById	proc_getSiteNames
proc_getSiteCount	

- Pour chaque base de données de contenu Web et base de données de contenu administrateur, affectez aux éléments sécurisables ci-dessous les droits d'exécution. (la liste exacte peut légèrement varier par rapport à l'environnement et les applications déployés dans la batterie SharePoint. Consultez l'observateur d'événements régulièrement pour affiner cette liste).


Éléments sécurisables	
proc_AddDocument	proc_GetLinkInfoSingleDoc
proc_AL	proc_ListAllWebsOfSite
proc_AddListItem	proc_ListUrls
proc_DeleteUrl	proc_SecUpdateUserActiveStatus
proc_DirtyDependents	proc_SecGetSiteGroupByTitle
proc_FetchDocForHttpGet	proc_SecGetUserPermissionOnGroup
proc_FetchDocForUpdate	proc_UpdateVirusInfo
proc_GetSiteFlags	proc_GetListMetaDataAndEventReceivers
proc_GetTpWebMetaDataAndListMetaData	proc_GetListFields
proc_GetUrlDocId	proc_UpdateDirtyDocument
proc_GetDocsMetaInfo	proc_UpdateListItem
proc_GetParentWebUrl	proc_SecGetIndividualUrlSecurityCheckEventReceivers
proc_GenerateNextId	UserData (sous la section Vues)
proc_GetWebMetaInfo	

- Pour chaque base de données de contenu Web et base de données de contenu de l'administrateur, affectez les droits d'exécution sur l'objet *fn_GetFullUrl* (Etape : Accédez à Programmabilité | Fonctions | Fonctions scalaires pour chaque base de données).

3 Aucune exigence pour l'appartenance au groupe d'administrateurs locaux.

SharePoint Server

- 1 Aucune exigence d'appartenance au groupe d'administrateurs locaux par le compte d'utilisateur de domaine (par exemple : MSMSDBAccnt) utilisé par McAfee Security for Microsoft SharePoint.
- 2 Aucune exigence pour la connexion interactive.
- 3 Aucune exigence pour l'administrateur de la collection de sites.

- 4 Créez un nouveau niveau de stratégie d'autorisation (par exemple : MSMS-Permissions) et accordez les autorisations suivantes. Ces autorisations sont le minimum pour que McAfee Security for Microsoft SharePoint travaille avec le modèle objet SharePoint et effectue une itération sur SharePoint Store pour une analyse et un nettoyage. (Les droits d'administrateur de la batterie SharePoint sont nécessaires pour opérer ce changement).
 - a Sous Autorisations de la collection de sites, accordez une autorisation Auditeur de collection de sites. Les auditeurs de collection de sites disposent d'un accès total en lecture à toute la collection de sites, notamment les autorisations de lecture et les données de configuration. McAfee Security for Microsoft SharePoint exige ceci car il surveille les paramètres antivirus SharePoint afin de déterminer si l'analyse en temps réel est activée ou désactivée.
 - b Dans la section des autorisations de liste, accordez les autorisations suivantes :
 - Gérer la liste : nécessaire pour remplacer/supprimer le contenu infecté ajouté en pièce jointe sous les éléments dans Discussions.
 - Remplacer l'extraction : nécessaire pour vérifier avec force un document détecté comme étant infecté et effectuer l'action conformément à la stratégie.
 - Ajouter des éléments : nécessaire pour remplacer le fichier infecté par un fichier contenant un message d'alerte de remplacement.
 - Modifier des éléments : nécessaire pour mettre à jour les documents extraits tout en archivant de force avec une vérification dans le commentaire.
 - Supprimer des éléments : nécessaire pour la suppression d'un élément de la liste infecté (document).
 - Afficher les éléments : requis pour le sélecteur de cible lors de la définition d'une cible d'analyse.
 - c Sous Autorisations des sites, accordez l'autorisation Afficher les pages - Afficher les pages dans une autorisation de site web. Autrement, McAfee Security for Microsoft SharePoint ne peut pas effectuer une itération sur le site dans les tâches d'analyse à la demande.
 - d Enregistrez le niveau de stratégie d'autorisation nouvellement créé.
 - 5 Pour chaque application Web créée dans la batterie SharePoint :
 - a Mettez à jour la stratégie d'application Web pour l'application Web respective afin d'ajouter le compte d'accès à la base de données du produit (par exemple : MSMSDBAcnt) avec le Niveau de stratégie d'autorisation créé précédemment (par exemple : MSMS-Permissions).
 - b Mettez à jour la stratégie d'application Web pour couvrir toutes les applications Web qui seront ajoutées à l'avenir.
- 
- Cela ne couvre pas l'application d'administration centrale - qui ne sera pas analysée à moins que l'option 1 ci-dessus ne soit choisie. Nous pouvons également ajouter le compte d'accès à la base du produit (par exemple : MSMSDBAcnt) comme compte d'administrateur de collection de sites secondaire sur l'application web d'administration centrale uniquement.
- 6 Des étapes manuelles peuvent être possibles pour les scripts. Des droits d'administrateur local ou GPO sont nécessaires pour effectuer ces mises à jour de groupe. Mettez à jour les groupes d'utilisateurs IIS et SharePoint (IIS_WPG (pour IIS 6) et IIS_IUSRS (IIS7) ou WSS_WPG) sur chaque serveur SharePoint Server en ajoutant le compte d'accès à la base de données McAfee Security for Microsoft SharePoint (par exemple : MSMSDBAcnt).
 - 7 L'autorisation d'ajout/modification permet au compte d'accès à la base de données du produit (par exemple : MSMSDBAcnt) d'accéder en lecture/suppression au dossier bin de McAfee Security for Microsoft SharePoint. (<Emplacement d'installation du produit>\Bin). (Des étapes manuelles

peuvent être possibles pour les scripts. Une autorisation administrateur local ou GPO est nécessaire pour effectuer les modifications). Ce dossier est propre à McAfee Security for Microsoft SharePoint. Par exemple : Pour l'installation par défaut, le chemin d'accès du dossier bin est C:\Program Files\McAfee\McAfee PortalShield\Bin



- Cette autorisation est requise si des analyses à la demande sont programmées via ePolicy Orchestrator. Lors de l'exécution, ePolicy Orchestrator passe les détails de configuration nécessaires pour l'analyse à la demande à l'agent plug-in McAfee, qui place les détails de configuration dans un fichier dans le dossier bin du produit avec une extension .tmp. Le processus à la demande (RunScheduled.exe) lit la configuration à partir de ce fichier puis le supprime.
- Si vous utilisez un compte de domaine standard (par exemple : MSMSDBAccnt), le compte n'aura pas d'accès en lecture/suppression pour le dossier bin. Ainsi l'accès en mode de modification doit être ajouté pour le compte d'accès à la base de données du produit (par exemple : MSMSDBAccnt) sur le dossier bin. Cette opération peut être effectuée après l'installation ou via GPO (Group Policy Objects).

B

Editeur de liste de sites Sitelist

L'option **Liste Sitelist** spécifie l'emplacement à partir duquel vous pouvez télécharger les mises à jour automatiques (y compris le fichier DAT et les moteurs d'analyse).

Editeur de liste de sites Sitelist

- A partir du menu **Démarrer**, cliquez sur **Programmes | McAfee | McAfee Security for Microsoft SharePoint | Editeur de liste de sites McAfee AutoUpdate**.

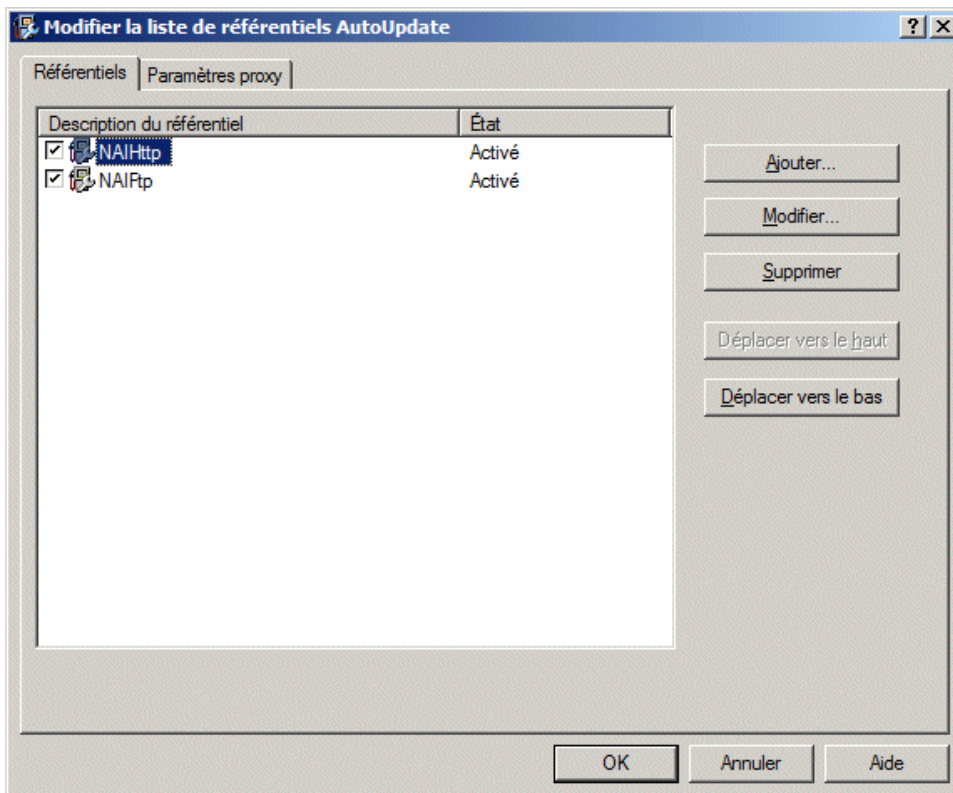


Figure B-1 Modifier la liste de référentiels AutoUpdate

Vous pouvez utiliser les onglets suivants :

- **Référentiels** : permet de configurer les paramètres de référentiel à partir desquels le logiciel peut télécharger les mises à jour automatiques.
Par défaut, McAfee Security for Microsoft SharePoint utilise une liste Sitelist pointant vers un site McAfee pour télécharger les mises à jour automatiques, mais vous pouvez également définir d'autres listes Sitelist pointant vers d'autres emplacements. Par exemple, vous avez peut-être copié les mises à jour automatiques dans un référentiel local et créé une liste Sitelist qui dirige vos systèmes logiciels vers ce référentiel local.
- **Paramètres proxy** : permet de configurer les paramètres de serveur proxy de sorte que le logiciel puisse se connecter à Internet via ce serveur afin de télécharger les mises à jour du produit.



Les paramètres appliqués dans l'Editeur de liste de sites SiteList sont enregistrés dans le fichier `SiteList.xml` situé dans le répertoire `C:\ProgramData\McAfee\Common Framework\`.

Sommaire

- [Configuration des paramètres de proxy Sitelist](#)
- [Configuration des paramètres de référentiel Sitelist](#)

Configuration des paramètres de proxy Sitelist

Configurez ces paramètres si votre organisation utilise un serveur proxy pour se connecter à Internet, afin que le logiciel puisse télécharger les mises à jour du produit.

Si votre organisation utilise des serveurs proxy pour la connexion à Internet, vous pouvez sélectionner l'option **Paramètres de proxy**.

Procédure

- 1 Cliquez sur **Démarrer | Programmes | McAfee | McAfee Security for Microsoft Exchange | Editeur de liste de sites McAfee Auto Update**.

La boîte de dialogue **Modifier la liste de référentiels AutoUpdate** s'affiche.

- 2 Cliquez sur l'onglet **Paramètres de proxy**.

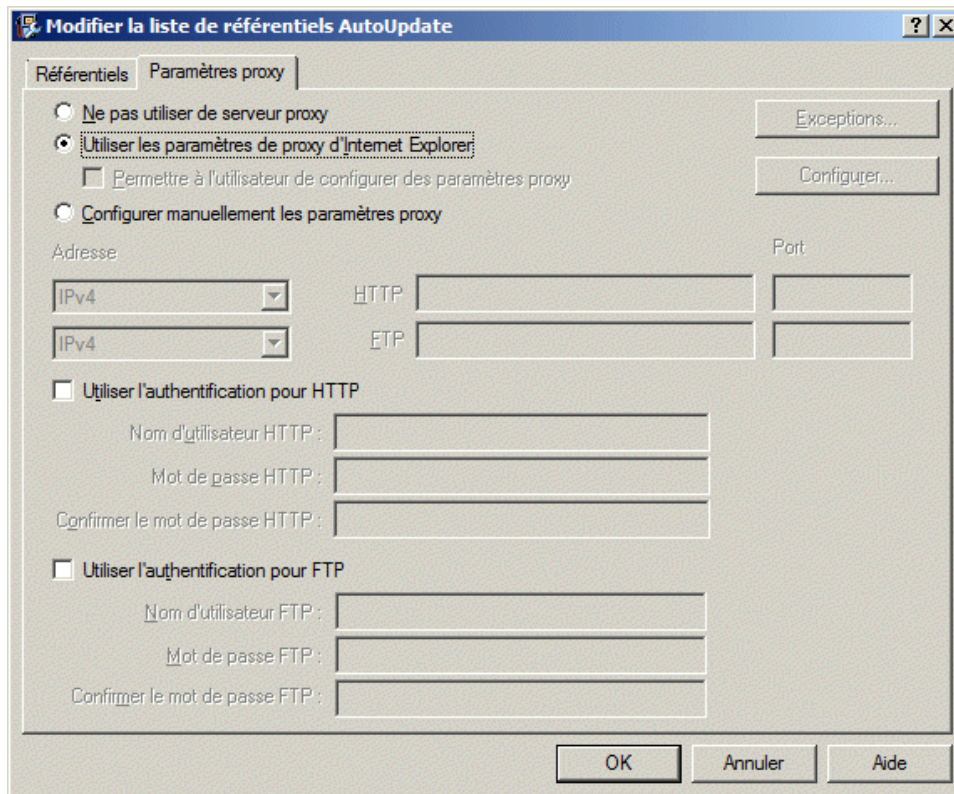


Figure B-2 Paramètres de proxy

- 3 Sélectionnez **Utiliser les paramètres du proxy** dans Internet Explorer ou **Configurer manuellement les paramètres du proxy** selon vos besoins.
- 4 Tapez l'adresse IP et le numéro de port du serveur HTTP ou FTP.
- 5 Vous pouvez utiliser les options suivantes :
 - **Utiliser l'authentification** — Permet d'activer l'authentification de l'utilisateur afin d'accéder au serveur proxy.
 - **Nom d'utilisateur** — Permet de spécifier un nom d'utilisateur à des fins d'authentification pour l'accès au serveur proxy.
 - **Mot de passe** — Permet de spécifier un mot de passe.
 - **Confirmez le mot de passe** — Permet de reconfirmer le mot de passe spécifié.
 - **Exceptions** — Permet au serveur proxy de contourner des domaines spécifiques. Cliquez sur **Exceptions**, puis sélectionnez **Préciser les exceptions** et indiquez les domaines à contourner.
- 6 Cliquez sur **OK**.

Configuration des paramètres de référentiel Sitelist

Le fichier de liste de sites **Sitelist** spécifie l'emplacement à partir duquel les mises à jour automatiques sont téléchargées.

Par défaut, McAfee Security for Microsoft SharePoint utilise une liste Sitelist pointant vers un site McAfee pour télécharger les mises à jour automatiques, mais vous pouvez également utiliser une liste Sitelist pointant vers d'autres emplacements. Par exemple, vous avez peut-être copié les mises à jour automatiques dans un référentiel local et créé une liste Sitelist qui dirige vos systèmes McAfee Security for Microsoft SharePoint vers ce référentiel local.

Procédure

- 1 Cliquez sur **Démarrer | Programmes | McAfee | Security for Microsoft Sharepoint | Editeur de liste de sites**. La boîte de dialogue **Modifier la liste de référentiels AutoUpdate** s'affiche.
- 2 Sous l'onglet **Référentiels**, cliquez sur **Ajouter**. La boîte de dialogue **Paramètres du référentiel** s'ouvre.

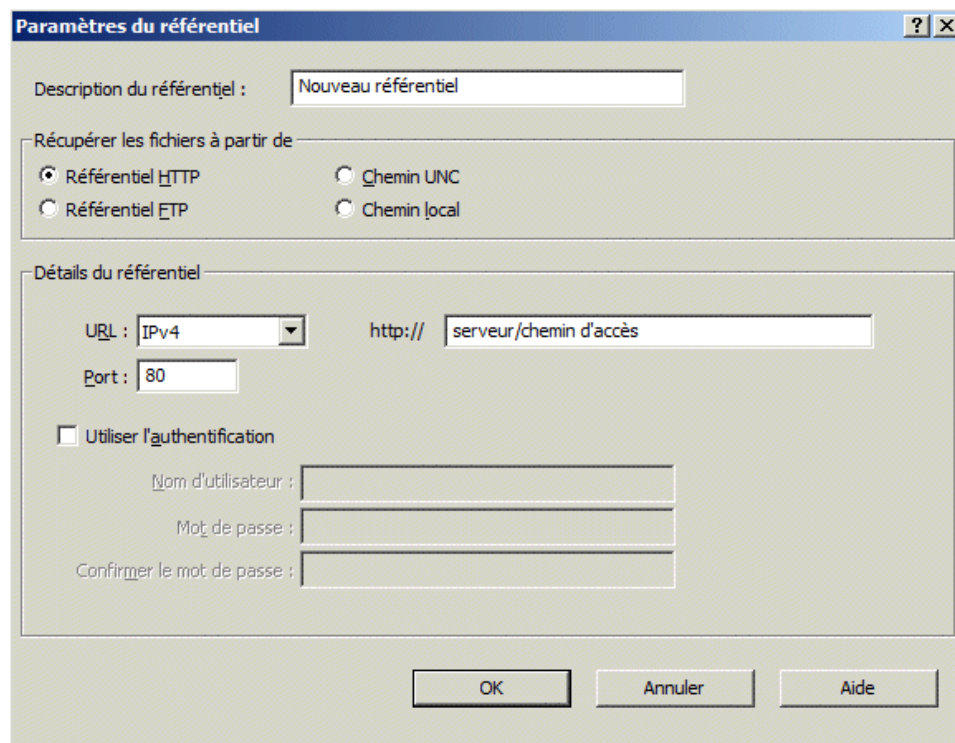


Figure B-3 Paramètres du référentiel

- 3 Sélectionnez l'une des options suivantes :
 - **Description du référentiel** — Permet de donner une brève description du référentiel.
 - **Récupérer les fichiers depuis** — Permet d'indiquer de quel type de référentiel extraire les fichiers. Les options disponibles sont **Référentiel HTTP**, **Référentiel FTP**, **Chemin UNC** et **Chemin local**.
 - **URL** — Permet d'indiquer l'URL du référentiel.
 - **Port** — Permet d'indiquer le numéro de port du référentiel.
 - **Utiliser l'authentification** — Permet d'activer l'authentification de l'utilisateur afin d'accéder au référentiel.
- 4 Spécifiez un nom d'utilisateur et un mot de passe pour l'authentification du référentiel et confirmez le mot de passe en le tapant de nouveau.

- 5 Cliquez sur **OK** pour ajouter le nouveau référentiel à la liste **Description du référentiel**.
- 6 Cliquez sur **OK** pour fermer la boîte de dialogue **Modifier la liste de référentiels AutoUpdate**.

C

Utilisation de la fonctionnalité de contrôle d'accès

Vous pouvez autoriser ou refuser l'accès de l'interface utilisateur de McAfee Security for Microsoft SharePoint à des utilisateurs ou des groupes précis.

- 1 Dans le menu **Démarrer**, cliquez sur **Programmes | McAfee | McAfee Security for Microsoft SharePoint | Contrôle d'accès**.
- 2 Sous **Noms de groupes ou d'utilisateurs**, sélectionnez l'utilisateur à qui vous souhaitez autoriser ou refuser l'accès à l'interface utilisateur du produit, puis cliquez sur **OK**.



- Le logiciel ajoute automatiquement les groupes d'utilisateurs Farm Administrator, Internet Information Services et Windows SharePoint Services à cette liste lors de l'installation.
- Le contrôle d'accès est utilisé à des fins internes par le logiciel pour établir des communications interprocessus (IPC, Inter-Process Communication). Ne supprimez pas les groupes d'utilisateurs Farm Administrator, Internet Information Services et Windows SharePoint Services de cette liste.

Index

A

- à la demande
 - analyse 28
- accès
 - Editeur de liste de sites Sitelist 117
- action à entreprendre
 - éléments détectés 42
- actions
 - à entreprendre 53
 - principaux 53
 - secondaires 53
- affichage
 - journaux du produit 85
- affichage des stratégies
 - avancé 46
 - héritage 46
- ajout
 - analyseur 51
 - filtre 51
- alerte
 - création 55
- alertes
 - configuration 55
- analyse à la demande 28
 - analyse avec reprise 31
 - analyse incrémentielle 31
 - création 31
 - planification 31
- analyseur
 - ajout 51
- analyseur antivirus
 - configuration des paramètres 64
- analyseur de base
 - gestion des paramètres 63
- analyseur de conformité et DLP
 - configuration des paramètres 68
- analyseurs 49
 - configuration 54
- analyseurs et filtres
 - liste 50
- avancé
 - affichage des stratégies 46

B

- base
 - analyseurs 49
 - filtres 49
- base de données locale
 - mise en quarantaine 76

C

- classement par ordre de priorité
 - stratégies 46
- composants installés 18
- composants supplémentaires 18
- configuration
 - alertes 55
 - analyseurs 54
 - paramètres à l'accès 89
 - paramètres de proxy Sitelist 118
 - paramètres de référentiel de Sitelist 120
 - Règles de conformité et DLP 58
 - règles de filtrage des fichiers 61
- configuration des paramètres
 - analyseur antivirus 64
 - analyseur de conformité et DLP 68
 - base de données locale 76
 - contenu chiffré 71
 - contenu corrompu 70
 - contenu protégé 71
 - contenu protégé par mot de passe 73
 - contenu signé 72
 - contrôle de l'analyseur 73
 - exportation 86
 - fichiers DAT 89
 - filtrage de fichiers 67
 - importation 86
 - provenant d'un autre serveur 87
- configuration existante
 - exportation 88
- configuration système requise 11
- contenu chiffré
 - configuration des paramètres 71
- contenu corrompu
 - configuration des paramètres 70

- contenu protégé
 - configuration des paramètres 71
- contenu protégé par mot de passe
 - configuration des paramètres 73
- contenu signé
 - configuration des paramètres 72
- contrôle de l'analyseur
 - configuration des paramètres 73
- création
 - nouvelle alerte 55
 - nouvelle règle 52
 - sous-stratégie 48
 - tâche d'analyse à la demande 31
- créer un compte d'utilisateur de domaine normal personnalisé: autorisations SQL minimales 113

D

- déni de service 34
- désinstaller le logiciel 95
- détection en temps réel 8
- diagnostic
 - configuration des paramètres 80
- diagramme
 - configuration des paramètres 79

E

- Editeur de liste de sites Sitelist
 - accès 117
 - paramètres de proxy 117
 - référentiel 117
- eicar 17
- éléments analysés
 - récemment 27
- éléments analysés récemment 27
- éléments détectés
 - action à entreprendre 42
 - configuration des paramètres 76
 - résultats de la recherche 42
- éléments mis en quarantaine
 - action à entreprendre 42
- exportation
 - configuration des paramètres 86
 - configuration existante 88

F

- filtre
 - ajout 51
 - gestion des paramètres 70
- filtre de fichiers
 - configuration des paramètres 67
- filtres 49
- filtres de recherche avancée 34
- filtres de recherche simples 33

- fonctionnalités
 - produit, fonctionnalités 7

G

- gérer à l'aide d'ePolicy Orchestrator
 - configuration système requise 97
- gestion
 - paramètres de filtre 70
 - paramètres de l'analyseur 63
- graphique
 - configuration des paramètres 79

H

- héritage
 - affichage des stratégies 46

I

- importation
 - configuration des paramètres 86
 - paramètres d'un autre serveur 87
 - Sitelist 86
- Informations
 - produit 26
- informations statistiques 19
- installation
 - désinstallation du produit 95
 - instructions d'installation 14
 - mise à niveau 16
 - pré-installation 11
 - réparation 93
 - test 16
- installation de SharePoint : dans une batterie 13
- instructions de pré-installation:mode serveur SharePoint unique 13
- introduction 7

J

- journal de débogage
 - configuration des paramètres 80
- journal des événements
 - configuration des paramètres 82
- journal du produit
 - configuration des paramètres 83
- journaux du produit
 - affichage 85

L

- licence
 - produit 25
- liste
 - analyseurs 50
 - filtres 50

M

- migration de stratégies
 - depuis ePolicy Orchestrator 98
- mime 34
- mise à jour
 - produit 25
 - version du produit 25

N

- nom de détection 34
- numéro de ticket 34

P

- paramètres
 - configuration de la base de données locale 76
 - configuration des diagnostics 80
 - configuration des éléments détectés 76
 - configuration des préférences de l'interface utilisateur 78
 - configuration du journal de débogage 80
 - configuration du journal des événements 82
 - configuration du journal du produit 83
 - configuration du service de génération de rapports d'erreur 82
 - configuration du tableau de bord 78
 - configuration pour les diagrammes 79
 - configuration pour les graphiques 79
- paramètres à l'accès, configuration 89
- paramètres de fichiers DAT
 - configuration 89
- paramètres de proxy
 - configuration de Sitelist 118
- paramètres de stratégie
 - gestion des analyseurs de base 63
 - gestion des filtres 70
- paramètres du référentiel
 - configuration de Sitelist 120
- plages horaires 62
- planification
 - tâche d'analyse à la demande 31
- préférences de l'interface utilisateur
 - configuration des paramètres 78
- principaux
 - actions 53
- principe de fonctionnement 8
- produit
 - licence 25
 - mise à jour 25
- produit, informations 26
- programme de compression 34
- programme potentiellement indésirable 34
- protection du serveur SharePoint 8

R

- rapports
 - graphiques 32
- rapports graphiques 32
- règle
 - création 52
- règles
 - Conformité et DLP 58
 - filtrage de fichiers 61
- Règles de conformité et DLP
 - configuration 58
- règles de filtrage des fichiers
 - configuration 61
- réparer l'installation 93
- ressource partagée 54
 - configuration d'alertes 55
 - configuration d'analyseurs 54
 - configuration de règles de conformité et DLP 58
 - configuration des règles de filtrage de fichiers 61
- rôles d'utilisateur 12

S

- secondaires
 - actions 53
- service de génération de rapports d'erreur
 - configuration des paramètres 82
- services 18
- Sitelist
 - importation 86
- sous-stratégie 47
- sous-stratégies
 - création 48
- Stratégie principale 47
- stratégies
 - classement par ordre de priorité 46
 - migration 98
 - tri 46

T

- tableau de bord
 - configuration des paramètres 78
- tâches post-installation 16
- test
 - analyseur à la demande 17
 - installation 16
- test de l'analyseur à l'accès 17
- tri
 - stratégies 46
- type d'analyse
 - analyse à la demande 28
- types
 - stratégie 47
- types d'analyse
 - à la demande 28

V

version

produit [25](#)

