Guide Produit

McAfee Security for Microsoft Exchange 8.6.0

Sommaire

1 Introduction

McAfee® Security for Microsoft Exchange (MSME) protège votre serveur Microsoft Exchange Server contre diverses menaces qui pourraient compromettre les ordinateurs, le réseau ou les employés.

MSME utilise l'analyse heuristique avancée contre les virus, le contenu indésirable, les programmes potentiellement indésirables et les types de fichier/messages interdits. Il analyse également les éléments suivants :

- Ligne d'objet et corps des e-mails
- Pièces jointes des e-mails (selon le type, le nom et la taille du fichier)
- Texte des pièces jointes aux e-mails
- URL dans le corps de l'e-mail

Enfin, le logiciel comprend le module complémentaire McAfee Anti-Spam qui protège Exchange Server contre les messages de spam et de phishing.

Sommaire

Fonctionnalités du produit

Les principales fonctionnalités de MSME sont décrites dans cette section.

- **Intégration de McAfee® Threat Intelligence Exchange (TIE) pour la vérification de la réputation des fichiers** : prend en charge la vérification de la réputation des fichiers TIE pour les pièces jointes aux e-mails. Cette fonction analyse rapidement les fichiers et prend des décisions avisées en validant la réputation des fichiers d'après les informations reçues en provenance de plusieurs sources connectées au serveur TIE dans votre environnement. Lorsque l'e-mail inclut un fichier compressé, les fichiers sont extraits et les fichiers dont le type est pris en charge sont envoyés pour la réputation TIE. Pour obtenir la liste des fichiers compressés pris en charge, reportez-vous à l'article KB89577.
- **Vérification de la réputation des fichiers par McAfee® Advanced Threat Defense** : MSME prend désormais en charge Advanced Threat Defense, une appliance en local qui permet de détecter et d'empêcher l'irruption de logiciels malveillants via TIE. Avec la protection Advanced Threat Defense, vous pouvez protéger vos systèmes contre les logiciels malveillants ''near-zero day'' et ''zero-day'' connus sans compromettre la qualité du service fourni aux utilisateurs de votre réseau.
- **Protection contre l'usurpation d'e-mails** : protège vos systèmes contre les e-mails d''usurpation.
- **Exclusion des e-mails volumineux de l'analyse** : vous pouvez maintenant exclure les e-mails de l'analyse à l'accès d'après leur taille.

- **Blocage des e-mails provenant d'adresses IP spécifiques** : vous pouvez maintenant ajouter une adresse IP spécifique ou une plage d'adresses IP dans la liste noire afin d'empêcher l'envoi d'e-mails à votre organisation à partir de cette ou de ces adresses IP, indépendamment de leur score de réputation.
- **Prise en charge de Microsoft Exchange 2016** : prend en charge Microsoft Exchange 2016, mise à jour cumulative (CU) 3 et versions ultérieures.
- **Prise en charge de Microsoft Windows Server 2016** : prend en charge le système d'exploitation Microsoft Windows Server 2016 64 bits.
- **Nouvelles versions de navigateur prises en charges** : Microsoft Internet Explorer 11.1066, Mozilla Firefox 54.0.1 et Google Chrome 59.0.3071.115.

Assurez-vous de désactiver le bloqueur de fenêtre pop-up dans les paramètres du navigateur pour accéder à l'interface Web du produit.

Autres fonctionnalités

- **Protection contre les virus** — Analyse tous les e-mails à la recherche de virus et protège votre serveur Exchange en interceptant, en nettoyant et en supprimant les virus détectés. MSME utilise des méthodes heuristiques avancées et identifie les virus inconnus ou les éléments de type viral suspectés afin de les bloquer.
- **Protection contre le spam** — Permet d'économiser de la bande passante et de l'espace de stockage, indispensables aux serveurs Exchange, en attribuant un score de spam à chaque e-mail lors de son analyse et en entreprenant des actions préconfigurées sur ces messages.
- **Protection contre le phishing** — Détecte les e-mails de phishing qui tentent d'obtenir frauduleusement vos données personnelles.
- **Protection contre les URL malveillantes** — Protège votre système contre les URL malveillantes. Une fois activé, MSME analyse chaque URL dans le corps de l'e-mail, obtient le score de réputation du lien, compare le lien au seuil défini, et effectue l'action adéquate par rapport à la configuration.
- **Capacité de détection des programmes de compression et des programmes potentiellement indésirables** — Détecte les programmes de compression qui compressent et chiffrent le code d'origine d'un fichier exécutable. Il détecte également les programmes potentiellement indésirables (PUP), logiciels écrits par des sociétés légitimes pour modifier l'état de sécurité ou de confidentialité d'un ordinateur.
- **Filtrage de contenu** — Analyse le contenu et le texte de la ligne de l'objet ou du corps d'un e-mail et d'une pièce jointe. MSME prend en charge le filtrage de contenu basé sur des expressions régulières (Regex).
- **Filtrage de fichiers** — Analyse une pièce jointe d'e-mail selon le nom, le type et la taille du fichier. MSME peut également filtrer les fichiers contenant du contenu chiffré, corrompu, protégé par mot de passe et signé numériquement.
- **Conformité et DLP** — Fonctionnalité garantissant que le contenu de l'e-mail est conforme aux stratégies de confidentialité et de conformité de votre organisation. Caractéristiques des 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, code source (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 pour la prévention des fuites de données.

- **Réputation de l'adresse IP** — Méthode de détection des menaces contenues dans les e-mails reposant sur l'adresse IP du serveur d'envoi. Le score de réputation de l'adresse IP reflète la probabilité de menace que pose une connexion réseau donnée. La fonctionnalité de réputation de l'adresse IP tire parti du service McAfee Global Threat Intelligence (GTI) en vue de prévenir les dommages et le vol de données en bloquant les e-mails au niveau de la passerelle, en fonction de l'adresse IP source du dernier serveur de messagerie. MSME traite le message avant qu'il ne pénètre dans l'organisation en rejetant ou en interrompant la connexion d'après le score de réputation de l'adresse IP.
- **Analyse à la demande avancée** — Capacité à exécuter des analyses à la demande de niveau granulaire sur Exchange Server 2010 et 2013, ce qui a pour effet d'accélérer ce type d'analyse. Vous pouvez planifier des analyses à la demande basées sur les filtres suivants : Objet, Pièces jointes, Expéditeur/Destinataire/Cc, Taille de l'e-mail, ID du message, Eléments non lus, et Durée.
- **Analyse en arrière-plan** — Facilite l'analyse de tous les fichiers dans la banque d'informations. Vous pouvez planifier l'analyse en arrière-plan de manière à analyser périodiquement un ensemble spécifique de messages au moyen des derniers moteurs et configurations d'analyse. Dans MSME, vous pouvez exclure des boîtes aux lettres de l'analyse.
- **Alertes sur l'intégrité du produit** — Ce sont des notifications concernant l'intégrité du produit. Vous pouvez configurer et planifier ces alertes.
- **Intégration dans McAfee ePolicy Orchestrator 5.1.x, 5.3.x et 5.9.x** : s'intègre à ePolicy Orchestrator 5.1.x, 5.3.x et 5.9.x pour fournir une méthode centralisée de gestion et de mise à jour de MSME sur tous les serveurs Exchange. Cela réduit la complexité d'administration et de mise à jour de divers systèmes, ainsi que le temps nécessaire pour effectuer ces opérations.
- **Interface utilisateur web** — Fournit une interface web conviviale basée sur DHTML.
- **Gestion des stratégies** — L'option de menu **Gestionnaire de stratégies**, disponible dans l'interface utilisateur du produit, répertorie les différentes stratégies que vous pouvez configurer et gérer au sein de MSME.
- **Analyseur centralisé, règles de filtre et paramètres d'alerte optimisés** — Grâce aux analyseurs, vous pouvez configurer les paramètres qu'une stratégie peut appliquer lors de l'analyse d'éléments. Les règles Filtrage de fichiers permettent de configurer des règles qui s'appliquent au nom, au type et à la taille de fichier.
- **Analyse et actions à la demande/temporelles** — Analyse les e-mails à des heures données ou à des intervalles réguliers.
- **Analyse Multipurpose Internet Mail Extensions (MIME)** — Norme de communication qui permet le transfert de formats non-ASCII via des protocoles, tels que SMTP, ne prenant en charge que les caractères ASCII 7 bits.
- **Quarantine Management** — Vous pouvez spécifier la base de données locale à utiliser comme référentiel pour mettre en quarantaine les e-mails infectés. Vous pouvez choisir d'enregistrer les messages mis en quarantaine sur votre propre serveur exécutant McAfee Quarantine Manager. C'est ce que l'on appelle la *quarantaine à distance*.
- **Mise à jour automatique de définitions de virus, de fichiers DAT supplémentaires, d'antivirus et de moteur antispam** — Fournit régulièrement des fichiers DAT mis à jour, des moteurs d'analyse antivirus et le moteur antispam pour détecter et nettoyer les dernières menaces.
- **Conservation et purge des anciens fichiers DAT** — Conserve les anciens fichiers DAT lors de périodes que vous définissez ou les purge le cas échéant.
- **Prise en charge de l'éditeur de liste de sites Sitelist** — Spécifiez un emplacement à partir duquel télécharger les mises à jour automatiques pour MSME.
- **Prise en charge de Small Business Server** — MSME est compatible avec les serveurs Small Business Server.

- **Rapports de détection** — Produit des rapports d'état et des rapports graphiques qui vous permettent d'afficher des informations concernant les éléments détectés.
- **Rapports de configuration** — Récapitulent la configuration du produit, notamment les informations relatives au serveur, à la version, au type et au statut de la licence, au produit, à la journalisation de débogage, aux paramètres à l'accès, aux stratégies à l'accès et aux stratégies de passerelle. Vous pouvez spécifier le moment où votre serveur doit envoyer le rapport de configuration à l'administrateur.
- **Détection des attaques par déni de service** : détecte les demandes ou attaques supplémentaires qui inondent et interrompent le trafic régulier sur un réseau. Une attaque par déni de service submerge sa cible de fausses demandes de connexion de sorte que la cible ignore les demandes légitimes. MSME considère les trois scénarios suivants comme des attaques par déni de service :
  - Le temps d'analyse dépasse le temps défini
  - Le niveau imbriqué dépasse le niveau défini
  - La limite de taille de fichier extensible des fichiers d'archive dépasse la taille définie
- **Notifications avancées** — Transférez les e-mails mis en quarantaine pour un audit de conformité à plusieurs utilisateurs en fonction de la catégorie de détection.
- Prise en charge de VMware Workstation 7.0 ou version ultérieure, et de VMware ESX 5.5.

Utilité de MSME

Votre organisation est vulnérable en raison des nombreuses menaces qui peuvent nuire à sa réputation, ses employés, ses ordinateurs et ses réseaux.

- La réputation d'une organisation peut être affectée par la perte d'informations confidentielles ou par un contenu choquant qui peut entraîner une action judiciaire.
- Diverses distractions électroniques et l'usage sans restrictions de l'e-mail et d'Internet peuvent affecter la productivité du personnel.
- Les virus et autres logiciels potentiellement indésirables peuvent endommager les ordinateurs et les rendre inutilisables.
- L'utilisation incontrôlée de divers types de fichiers sur vos réseaux peut entraîner des problèmes de performance pour votre organisation entière.

Menaces pesant sur votre organisation

Prenez connaissance des diverses menaces pouvant avoir des répercussions sur une organisation.

Type de menace	Description
Réputation d'une société	Une remarque infondée ou mal renseignée d'un employé pourrait poser des problèmes juridiques, si elle n'est pas couverte par une clause d'exclusion de responsabilité.
Spam (e-mail non sollicité)	Les e-mails commerciaux non sollicités sont l'équivalent électronique du spam ou du courrier indésirable. Ils contiennent souvent des publicités non sollicitées par les destinataires. Bien qu'il constitue plus une gêne qu'une menace, le spam peut réduire les performances de votre réseau.
E-mails volumineux	Les e-mails ou les messages qui contiennent de nombreuses pièces jointes peuvent ralentir les performances des serveurs de messagerie.
Virus de mass-mailing	Bien qu'ils puissent être nettoyés comme n'importe quel autre virus, ils peuvent se propager rapidement et réduire les performances de votre réseau.

Type de menace	Description
E-mails émanant de sources indésirables	D'anciens employés mécontents ou des individus peu scrupuleux qui connaissent l'adresse e-mail de certains membres de votre personnel peuvent vous créer des problèmes en envoyant des e-mails indésirables.
Utilisation non professionnelle des e-mails	Si la plupart des employés utilisent les adresses e-mail de destinataires hors de leur organisation, c'est dans la plupart des cas pour des raisons personnelles ou non professionnelles.
Fuite d'informations confidentielles d'une société	Les employés peuvent révéler des informations confidentielles concernant des produits non distribués, des clients ou des partenaires.
Langage choquant	Des mots ou des expressions choquants peuvent apparaître dans les e-mails et les pièces jointes. Outre leur aspect choquant, ils peuvent être à l'origine d'une action judiciaire.
Transfert de fichiers de divertissement	Les fichiers vidéo ou audio volumineux destinés au divertissement peuvent réduire les performances du réseau.
Types de fichier inefficaces	Certains fichiers utilisent de grandes quantités de mémoire et peuvent être lents au transfert, mais des alternatives sont souvent disponibles. Par exemple, les fichiers GIF et JPEG sont beaucoup plus petits que leurs fichiers équivalents BMP.
Transfert de fichiers volumineux	Le transfert de fichiers volumineux peut réduire les performances du réseau.
Attaque par déni de service	Une augmentation subite du nombre de fichiers volumineux peut sérieusement affecter les performances de votre réseau, ce qui le rend inutilisable pour ses utilisateurs légitimes. Pendant l'analyse des fichiers compressés de grande taille, MSME considère ces trois paramètres comme une attaque de déni de service : • Le temps d'analyse des fichiers compressés dépasse le seuil. • Les niveaux imbriqués des fichiers compressés sont identifiés. Par exemple, un fichier .zip compressé contient un autre fichier compressé, et continue de s'étendre avec plus de fichiers compressés. • La limite de taille extensible des fichiers archivés dépasse le seuil.
Texte pornographique	Le langage ou les termes vulgaires ne doivent pas être utilisés dans les e-mails.
Virus et autres logiciels potentiellement indésirables	Les virus et autres logiciels potentiellement indésirables peuvent rapidement rendre des ordinateurs et des données inutilisables.
Contenu corrompu ou chiffré	Ce type de contenu ne peut pas être analysé. Des stratégies adéquates doivent être configurées pour le gérer.

Procédure de protection d'Exchange Server par MSME

Familiarisez-vous avec la manière dont MSME protège Exchange Server en accédant à tous les e-mails qui atteignent le serveur et tous ceux qui sont lus depuis la boîte aux lettres et écrits vers cette dernière.

Protection de votre serveur Microsoft Exchange Server

MSME utilise l'interface d'analyse antivirus du serveur Exchange pour obtenir un accès total à tous les e-mails lus depuis la boîte aux lettres du serveur et écrits vers elle.

- Le moteur d'analyse antivirus compare l'e-mail à toutes les signatures de virus connues enregistrées dans les fichiers DAT.
- Le moteur de gestion de contenu recherche dans l'e-mail du contenu interdit tel que spécifié dans les stratégies de gestion de contenu de MSME.

Si ces vérifications permettent d'identifier des virus ou du contenu interdit dans l'e-mail, MSME entreprend l'action indiquée. Si aucun élément n'est détecté, MSME transmet à nouveau les informations à l'interface d'analyse antivirus afin de terminer la demande de message d'origine dans Microsoft Exchange.

Détection en temps réel

MSME s'intègre dans votre serveur Exchange et fonctionne en temps réel pour détecter et supprimer les virus ou tout autre code nuisible ou indésirable. Il garantit également un environnement sain en analysant les bases de données sur le serveur Exchange. Chaque fois qu'un e-mail est envoyé ou reçu d'une source, MSME le compare à une liste de virus connus et de comportements de type viral suspects, puis intercepte et nettoie le fichier infecté avant qu'il ne s'étende. Il peut également analyser le contenu de l'e-mail (et de ses pièces jointes) à l'aide des règles et des stratégies définies dans le logiciel.

Analyse des e-mails

- Les moteurs d'antispam, d'antivirus et de gestion de contenu analysent les messages électroniques et fournissent le résultat à MSME avant que le contenu ne soit écrit dans le système de fichiers ou lu par les utilisateurs de Microsoft Exchange.
- Les moteurs d'analyse antivirus et antispam comparent l'e-mail à toutes les signatures connues enregistrées dans les fichiers de définition de virus (DAT) et dans les règles antispam installés. Le moteur antivirus analyse également le message à l'aide des méthodes heuristiques de détection sélectionnées.
- Le moteur de gestion de contenu recherche dans l'e-mail du 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 le message, MSME transmet l'information de nouveau à Microsoft Exchange. En cas de détection, MSME agit comme défini dans ses paramètres de configuration.

Comment l'analyse fonctionne-t-elle ?

- Le moteur d'analyse et les fichiers DAT sont les éléments centraux de MSME. Le moteur est un analyseur de données complexes. Les fichiers DAT contiennent de nombreuses informations dont des milliers de pilotes différents, chacun contenant des instructions détaillées sur la façon d'identifier un virus ou un type de virus.
- Le moteur d'analyse fonctionne avec les fichiers DAT. Il identifie le type d'élément analysé et décode le contenu de cet objet afin de comprendre de quoi il s'agit. Il utilise ensuite les informations contenues dans les fichiers DAT pour rechercher et localiser les virus connus. Chaque virus a une signature distinctive. Chaque virus possède une séquence de caractères unique et le moteur recherche cette signature. Il fait appel à une technique appelée « analyse heuristique » pour rechercher les virus inconnus. Celle-ci consiste à analyser le code du programme de l'objet et à rechercher des caractéristiques distinctives des virus.
- Une fois que le moteur a confirmé l'identité d'un virus, il nettoie l'objet dans la mesure du possible. Par exemple, il supprime une macro infectée d'une pièce jointe ou supprime le code de virus dans un fichier exécutable.

Que doit-on analyser et quand ?

- La menace constituée par les virus peut venir de nombreuses sources telles que des macros infectées, des fichiers de programme partagés, des fichiers partagés sur un réseau, des messages électroniques et des pièces jointes, des disquettes, des fichiers téléchargés sur Internet, etc. Les différents produits logiciels antivirus McAfee Security visent des zones de vulnérabilité précises. Il est conseillé d'adopter une approche à plusieurs niveaux pour bénéficier de toutes les fonctionnalités de détection antivirus, de sécurité et de nettoyage nécessaires.
- MSME 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, en particulier par les e-mails et l'accès à Internet.
- Vous pouvez configurer ou activer les diverses actions qui vous permettent de déterminer comment votre serveur MSME doit gérer différents éléments et les mesures qu'il doit prendre sur les éléments détectés ou suspects.

Procédure d'analyse des e-mails

MSME n'analyse pas de la même manière les e-mails entrants, sortants et internes.

Chaque fois qu'un e-mail est envoyé à une destination ou reçu de la part d'une source, MSME l'analyse en le comparant à une liste de virus connus et de comportements suspectés viraux. MSME peut également analyser le contenu de l'e-mail en s'appuyant sur des règles et des stratégies définies au sein du logiciel.

Lorsque MSME reçoit un e-mail, il l'analyse dans cet ordre :

1. Réputation des adresses IP
2. Antispam ou phishing
3. Anti-usurpation
4. Contenu corrompu ou chiffré
5. Filtre des fichiers
6. Analyse de contenu (Conformité et DLP)
7. Analyse antivirus
8. Réputation de l'URL de courrier

Même si les e-mails sont analysés dans cet ordre, lorsqu'un élément est d'abord détecté par l'analyseur de filtrage de fichiers, il est tout de même soumis à une analyse antivirus avant d'être mis en quarantaine.

Vous pouvez détecter un e-mail d'après son adresse IP source si vous activez la fonctionnalité MSME de réputation des adresses IP. Cette fonctionnalité est disponible si vous avez installé le composant McAfee Anti-Spam.

Analyse des e-mails entrants

Cette section présente des informations détaillées sur les étapes qu'entraîne l'arrivée d'un e-mail dans votre organisation et sur la manière dont MSME analyse ce message afin de déterminer s'il est infecté ou pas.

Le processus décrit ci-après part de l'hypothèse selon laquelle vous avez installé MSME pour tous les rôles suivants dans votre organisation.

Microsoft Exchange Server 2010 :

- Serveur de transport Edge
- Serveur de transport Hub
- Serveur de boîte aux lettres

Microsoft Exchange Server 2013 et 2016 :

- Serveur de transport Edge
- MBX

Si vous ne disposez d'aucun serveur Exchange pour le rôle Transport Edge ou Transport Hub, MSME ignore les étapes liées à ce rôle.

Procédure

1. La pile SMTP hébergée par `EdgeTransport.exe` dans le rôle serveur de transport Edge reçoit l'e-mail.
2. MSME IP Agent (McTxIPAgent) vérifie la réputation de l'adresse IP source. La vérification par IP Agent a lieu avant les opérations TxAgent.
3. MSME Transport Agent (McAfeeTxAgent) analyse l'e-mail et vérifie qu'il ne contient aucun spam ni aucun message de phishing et que sa taille est correcte.
4. En cas de détection positive, l'e-mail est supprimé ou renvoyé à la pile SMTP.
5. Si l'e-mail n'est pas infecté, McAfeeTxRoutingAgent procède à son traitement.
6. MSME reçoit le même flux et lance une analyse de type filtrage des fichiers, analyse de contenu, analyse antivirus (AV) et filtrage des URL.
7. En cas de détection positive, une action est entreprise en fonction de la configuration du produit.
8. MSME estampille l'e-mail avec la référence antivirus (AV) conformément aux spécifications Microsoft.
9. L'e-mail est à présent envoyé au rôle serveur de transport Hub Exchange.
10. La pile SMTP hébergée par `EdgeTransport.exe` dans le rôle serveur de transport Hub reçoit l'e-mail.
11. L'agent de transport MSME (McAfeeTxAgent) analyse l'e-mail afin de déterminer s'il s'agit d'un message de spam ou de phishing, ou pour vérifier sa taille. Ce n'est que dans le cas de la tâche EdgeSync (serveur Edge ou Hub) que la session est authentifiée lorsque l'analyse antispam est ignorée. Dans ce cas, la vérification du créateur est utilisée pour l'authentification de la session.
12. En cas de détection positive, l'e-mail est supprimé ou renvoyé à la pile SMTP.
13. Si l'e-mail n'est pas infecté, McAfeeTxRoutingAgent le traite et recherche la référence antivirus.
14. Si une référence AV est présente, il la vérifie et la compare à celle que MSME constitue avec le moteur/le fichier DAT dans le rôle serveur de transport Hub.
15. Si la référence est différente, MSME reçoit le même flux et procède à différentes analyses : filtrage de fichiers, analyse du contenu et analyse antivirus.
16. Lors de l'analyse du trafic, MSME recherche une référence AV tandis que dans une analyse VSAPI, c'est la banque d'informations Exchange qui se charge de cette tâche et MSME ne reçoit pas d'appel d'analyse en cas de correspondance de référence antivirus.
17. En cas de détection positive, une action est entreprise en fonction de la configuration du produit.
18. MSME estampille l'e-mail avec la référence antivirus (AV) conformément aux spécifications Microsoft.
19. L'e-mail est acheminé jusqu'au rôle serveur de boîte aux lettres Exchange.
20. La banque d'informations Exchange reçoit l'e-mail et recherche la référence antivirus avant de l'enregistrer dans sa base de données.
21. En cas de correspondance de la référence AV, la banque d'informations enregistre l'élément sans l'analyser.

22 Si la référence AV ne correspond pas, la banque d'informations Exchange appelle VSAPI (Virus Scanning API) et analyse l'e-mail.

> La vérification VSAPI s'applique uniquement aux serveurs Microsoft Exchange 2010.

23 En cas de détection d'un élément non autorisé, l'e-mail est remplacé ou supprimé conformément à la configuration du produit.

> Les rôles Transport Hub et de boîte aux lettres ne sont pas applicables pour Microsoft Exchange Server 2013 et 2016.

Analyse des e-mails sortants

Cette section présente des informations détaillées sur les étapes qu'entraîne l'envoi d'un e-mail à l'extérieur de votre organisation et sur la manière dont MSME analyse ce message afin de déterminer s'il est infecté ou pas.

Procédure

1 L'utilisateur final envoie un e-mail à un utilisateur externe à l'aide du client de messagerie.

2 La banque d'informations Exchange reçoit l'e-mail et l'analyse dans le dossier Boîte d'envoi.

3 En cas de détection positive, l'e-mail est remplacé ou supprimé en fonction de la configuration du produit. S'il est remplacé, il est soumis à la file d'attente de transport.

4 La pile SMTP hébergée par `EdgeTransport.exe` dans les rôles Hub/MBX reçoit l'e-mail.

5 MSME Transport Agent (McAfeeTxRoutingAgent) soumet l'e-mail à une analyse de type filtrage des fichiers, analyse de contenu, analyse antivirus, analyse de la réputation de l'URL et ajout d'une clause d'exclusion de responsabilité.

6 En cas de détection positive, l'e-mail est supprimé ou remplacé et renvoyé comme il convient à la pile SMTP.

7 Si l'e-mail n'est pas infecté, il est renvoyé à la pile SMTP pour poursuivre son acheminement.

8 Si l'e-mail est acheminé jusqu'au rôle serveur Edge à partir de ce serveur Hub, alors :

   a La pile SMTP hébergée par `EdgeTransport.exe` dans le rôle serveur de transport Edge reçoit l'e-mail.

   b L'agent de transport MSME (McAfeeTxRoutingAgent) recherche la référence antivirus (le cas échéant).

   c Si une référence AV est présente, il la vérifie et la compare à celle que MSME constitue avec le moteur/le fichier DAT dans le rôle serveur de transport Edge.

   d Si la référence est différente, MSME reçoit le même flux et effectue une analyse de type filtrage des fichiers, analyse de contenu, analyse antivirus, puis analyse de la réputation de l'URL.

   e En cas de détection positive, une action est entreprise en fonction de la configuration du produit.

   f MSME estampille l'e-mail avec la référence antivirus (AV) conformément aux spécifications Microsoft pour le rôle serveur de transport Edge.

9 L'e-mail est alors renvoyé à la pile SMTP, hébergée par `EdgeTransport.exe` dans le rôle serveur de transport Edge, pour poursuivre son acheminement.

Analyse des e-mails internes

Cette section présente des informations détaillées sur les étapes qu'entraîne l'envoi d'un e-mail au sein de votre organisation et sur la manière dont MSME analyse ce message afin de déterminer s'il est infecté ou pas.

Procédure

1. L'utilisateur final envoie un e-mail à un utilisateur interne à l'aide du client de messagerie.
2. Dans Exchange Server 2010, l'e-mail est reçu et analysé dans le dossier Boîte d'envoi. Dans Exchange Server 2013 et 2016, les e-mails sont redirigés vers la file d'attente Transport du dossier Boîte d'envoi.
3. En cas de détection positive, l'e-mail est remplacé ou supprimé en fonction de la configuration du produit. S'il est remplacé, il est soumis à la file d'attente de transport.
4. La pile SMTP hébergée par `EdgeTransport.exe` dans le rôle serveur de transport Hub reçoit l'e-mail.
5. L'agent de transport MSME (McAfeeTxRoutingAgent) procède à différentes analyses : filtrage de fichiers, analyse du contenu et analyse antivirus.
6. En cas de détection positive, l'e-mail est supprimé ou remplacé et renvoyé comme il convient à la pile SMTP.
7. MSME estampille l'e-mail avec la référence antivirus (AV) conformément aux spécifications Microsoft pour le rôle serveur de transport Hub.
8. Si l'e-mail n'est pas infecté, il est renvoyé à la pile SMTP pour poursuivre son acheminement.
9. Le serveur de boîtes aux lettres Exchange reçoit l'e-mail.
10. La banque d'informations Exchange vérifie la référence AV et, en cas de correspondance, l'e-mail n'est pas envoyé pour analyse MSME via une analyse VSAPI ; il est soumis à une analyse de type analyse antivirus, analyse de la réputation de l'URL, filtrage des fichiers et analyse de contenu par VSAPI.

2 Tableau de bord

Le tableau de bord organise et présente les informations de manière lisible et facilement compréhensible.

Le tableau de bord MSME contient des informations critiques concernant le niveau de protection du serveur contre le spam, le phishing, les virus, les programmes potentiellement indésirables, les URL malveillantes et tout autre contenu indésirable. 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), aux informations de licence du produit et aux éléments analysés récemment.

Sommaire

Informations statistiques des éléments détectés

Affiche des informations détaillées sur le nombre total d'e-mails analysés par MSME et le nombre d'e-mails 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.

L'onglet **Statistiques** comprend les sections suivantes :

- **Détections**
- **Analyse**
- **Graphique**

Cliquez sur **Réinitialiser** pour effacer les informations statistiques de tous les compteurs dans la section **Détections** et réinitialiser leur valeur sur zéro. La réinitialisation des statistiques n'entraîne pas la suppression des éléments mis en quarantaine sous **Eléments 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** | **Eléments 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 **Eléments 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'e-mails analysés par MSME 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'e-mails et de documents qui déclenchent l'une des méthodes de détection. Par exemple, si un e-mail contient deux pièces jointes infectées par un virus, les statistiques associées à la catégorie **Virus** sont incrémentées d'une unité, et non de deux. Les statistiques de génération de rapports sont établies à partir des e-mails plutôt que des fichiers individuels ou des détections. Elles sont plus intuitives dans un environnement de serveur de messagerie.

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

Tableau 2-1 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 sont disponibles dans le graphique.
	Indique que les statistiques de la catégorie de détection concernée ne sont pas disponibles dans le graphique.

Les icônes graphiques et s'affichent uniquement lorsque l'option <**Sélectionner des détections**> est sélectionnée dans la liste déroulante **Graphique**.

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

Tableau 2-2 Définition des catégories de détection

Catégorie	Informations supplémentaires	Description
Nettoyer	Si le flux de la messagerie contient davantage d'e-mails non infectés que les détections, l'activation de l'icône pour les e-mails non infectés peut supprimer le graphique d'autres catégories. Dans ce type de scénario, désactivez l'icône en regard de la catégorie **Non infecté**.	Désigne les e-mails légitimes ne représentant aucune menace pour l'utilisateur et ne déclenchant aucun des analyseurs MSME.
Spam	Ce compteur est uniquement disponible si le module complémentaire McAfee Anti-Spam est installé.	Désigne un e-mail non sollicité généralement envoyé en masse à de nombreux destinataires qui n'avaient pas demandé à le recevoir et ne s'étaient pas inscrits pour le recevoir.

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

Catégorie	Informations supplémentaires	Description
	Analysé par l'analyseur antispam	Comprend tous les e-mails soumis à une analyse antispam par MSME.
	Détecté comme spam	Comprend les e-mails identifiés comme spam mais non mis en quarantaine en raison des paramètres de stratégie.
	Bloqué comme spam	Comprend les e-mails identifiés comme spam et mis en quarantaine en raison des paramètres de stratégie.
Phishing	Ce compteur est disponible uniquement si le module complémentaire McAfee Anti-Spam est installé.	Le phishing est une méthode utilisée pour obtenir des informations personnelles par des moyens frauduleux ou déloyaux. Ces informations personnelles peuvent comprendre vos numéros de carte de crédit, mots de passe et informations de connexion à vos comptes bancaires. Ces e-mails imitent des sources approuvées, telles que des banques et des sociétés légitimes. En général, ces e-mails vous invitent à cliquer sur un lien pour vérifier ou mettre à jour des informations personnelles. Comme le spam, les e-mails de phishing sont envoyés en masse.
	Phishing détecté	Comprend les e-mails identifiés comme des messages de phishing (hameçonnage) mais non mis en quarantaine en raison des paramètres de stratégie.
	Phishing bloqué	Comprend les e-mails identifiés comme des messages de phishing (hameçonnage) et mis en quarantaine en raison des paramètres de stratégie.
E-mails falsifiés	Ce compteur est disponible uniquement si le module complémentaire McAfee Anti-Spam est installé.	
	Erreur matérielle SPF détectée	E-mails identifiés comme des e-mails falsifiés de type Erreur matérielle.
	Erreur logicielle SPF détectée	E-mails identifiés comme des e-mails falsifiés de type Erreur logicielle.
Réputation de l'adresse IP	Ce compteur est disponible uniquement si le module complémentaire McAfee Anti-Spam est installé.	Méthode de détection des menaces contenues dans les e-mails reposant sur l'adresse IP du serveur d'envoi. Le score de réputation de l'adresse IP reflète la probabilité de menace que pose une connexion réseau donnée. La fonctionnalité de réputation de l'adresse IP tire parti du service McAfee Global Threat Intelligence (GTI) en vue de prévenir les dommages et le vol de données en bloquant les e-mails au niveau de la passerelle, en fonction de l'adresse IP source du dernier serveur de messagerie. MSME traite le message avant qu'il ne pénètre dans l'organisation en rejetant ou en interrompant la connexion d'après le score de réputation de l'adresse IP.
	Adresse IP détectée	Comprend tous les e-mails qui atteignent le serveur MSME.
	Adresse IP abandonnée	Comprend les e-mails mis en quarantaine par MSME en raison de la fonctionnalité de réputation de l'adresse IP. Dans ce cas, l'expéditeur n'est pas informé du statut de remise du courrier électronique.

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

Catégorie	Informations supplémentaires	Description
	Adresse IP rejetée	Comprend les e-mails mis en quarantaine par MSME en raison de la fonctionnalité de réputation de l'adresse IP. Dans ce cas, l'expéditeur est informé du statut de remise du courrier électronique.
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 détectés	Virus détecté dans un e-mail entrant et pour lequel une action appropriée est entreprise en fonction des paramètres de stratégie.
	Virus nettoyés	Virus supprimé d'un e-mail entrant et pour lequel une action appropriée est entreprise en fonction des paramètres de stratégie.
Détections TIE et ATD	**Réputations des fichiers**	Pièces jointes dont le type de fichier est pris en charge et qui sont envoyées au serveur TIE pour vérification de la réputation des fichiers.
	Réputations des certificats	Pièces jointes dont le type de fichier est signé et pris en charge et qui sont envoyées au serveur TIE pour vérification de la réputation des certificats.
	Envois ATD	Pièces jointes dont le type de fichier est pris en charge et qui sont envoyées au serveur ATD pour vérification de la réputation d'après la catégorie d'acceptation et la taille de fichier sélectionnées.
	Total de détections TIE	Pièces jointes dont le type de fichier est pris en charge et dont la réputation a été vérifiée par TIE.
Programmes potentiellement indésirables		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	Programme potentiellement indésirable détecté dans un e-mail entrant et pour lequel une action appropriée est entreprise en fonction des paramètres de stratégie.
	Programme potentiellement indésirable bloqué	Programme potentiellement indésirable supprimé d'un e-mail entrant et pour lequel une action appropriée est entreprise en fonction des paramètres de stratégie.
Types de fichiers et messages interdits		Certains types de pièce jointe sont susceptibles d'être des virus. Le blocage des pièces jointes en fonction de leur extension de fichier offre à votre système de messagerie un niveau de sécurité supplémentaire. Les messages et les types de fichier interdits sont tous recherchés dans les e-mails internes et externes.

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

Catégorie	Informations supplémentaires	Description
	Types de fichiers interdits	Certains types de pièce jointe sont susceptibles d'être des virus. Le blocage des pièces jointes en fonction de leur extension de fichier offre à votre système de messagerie un niveau de sécurité supplémentaire.
	Messages interdits	Comprend les e-mails dont vous souhaitez interdire l'accès à votre système de messagerie. Le contenu interdit est recherché à la fois dans les e-mails internes et externes.
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**.	Arrêtez la fuite de données confidentielles par e-mail. MSME offre une fonctionnalité d'analyse de contenu des e-mails 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. Favorisez la prévention des fuites de données en utilisant Data Loss Prevention (DLP), la solution de protection de messagerie 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.
Contenu indésirable		Un contenu indésirable désigne tout contenu que l'utilisateur ne souhaite pas recevoir par e-mail. Il est possible de définir les règles au moyen de certains mots ou expressions qui déclenchent ensuite une stratégie correspondante et bloquent l'e-mail.
	Programmes de compression	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 sont spécialement conçus pour contourner les logiciels de sécurité et éviter l'ingénierie inverse.
	Contenu chiffré/corrompu	Comprend les e-mails qu'il n'est pas possible de classer comme contenant des données chiffrées ou corrompues.
	Contenu chiffré	Certains e-mails sont chiffrés, ce qui implique que leur contenu ne peut pas être analysé. Les stratégies de contenu chiffré déterminent le mode de gestion des e-mails chiffrés lors de leur détection.

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

Catégorie	Informations supplémentaires	Description
	Contenu signé	Lorsque vous envoyez des informations par voie électronique, elles risquent d'être altérées, accidentellement ou délibérément. Certains logiciels de messagerie ont donc recours à des signatures numériques, forme électronique d'une signature manuscrite. Une signature numérique consiste en des données supplémentaires ajoutées à un message, qui identifient et authentifient l'expéditeur, de même que les informations contenues dans le message. Elle est chiffrée et joue en quelque sorte le rôle de synthèse unique des données transmises. En règle générale, il s'agit d'une longue chaîne de lettres et de chiffres figurant au bas d'un message reçu. Le logiciel de messagerie réexamine les informations contenues dans le message de l'expéditeur et crée une signature numérique. Si la signature est identique à celle d'origine, cela signifie que les données n'ont pas été modifiées. 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. L'e-mail est toujours accessible en lecture mais la signature numérique d'origine est « rompue ». Le destinataire ne peut pas se fier au contenu du message, car celui-ci a peut-être été altéré d'autres façons.
	Contenu corrompu	Le contenu de certains e-mails peut être corrompu et, par conséquent, il ne peut pas être analysé. Les stratégies de contenu corrompu déterminent le mode de gestion des e-mails en cas de détection d'un contenu corrompu.
	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 e-mails est protégé et, par conséquent, il ne peut pas être analysé. Les stratégies de contenu protégé déterminent le mode de gestion des e-mails en cas de détection d'un contenu protégé.
	Fichiers protégés par mot de passe	Il est possible de protéger au moyen d'un mot de passe les fichiers envoyés par e-mail. Il n'est pas possible d'analyser les fichiers protégés par mot de passe. Des stratégies spécifient comment traiter les e-mails qui contiennent un fichier protégé par mot de passe.

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

Catégorie	Informations supplémentaires	Description
	Messages MIME incomplets	Le standard de communication MIME (Multipurpose Internet Mail Extensions) permet de transférer des formats non ASCII via des protocoles, dont 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. Si le contenu du corps d'un message MIME est trop volumineux pour passer à travers le système de transfert d'e-mails, il peut être scindé en plusieurs messages MIME de taille plus petite. Ces messages MIME sont appelés messages MIME partiels ou incomplets, car chaque message MIME ne contient qu'un fragment du message total à transmettre.
Réputation de l'URL de courrier	**URL détectées**	URL suspectes détectées dans les e-mails par la fonction Réputation de l'URL.

Planification d'une mise à jour logicielle

Maintenez à jour votre logiciel avec la dernière version des fichiers DAT de l'antivirus, du moteur antivirus et des pilotes supplémentaires en planifiant une mise à jour automatique.

Par défaut, la fréquence de mise à jour du produit est fonction des paramètres de référentiel spécifiés dans l'**éditeur SiteList**. Pour modifier les paramètres de référentiel, faites appel à **l'éditeur SiteList**, accessible via **Démarrer** | **Tous les programmes** | **McAfee** | **Security for Microsoft Exchange**. Cependant, si votre ordinateur est managé par un serveur ePolicy Orchestrator, la mise à jour du produit dépend des paramètres configurés dans ePolicy Orchestrator.

Procédure

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 Sous **Fréquence des mises à jour**, cliquez sur **Modifier la planification**.

La page **Modifier la planification** s'affiche.

4 Sous **Choisir une heure**, sélectionnez une option en fonction de la fréquence de mise à jour du logiciel nécessaire.

Comme meilleure pratique, il est conseillé de planifier une mise à jour quotidienne, en sélectionnant **Jours** et en précisant `1` dans la zone de texte **Tou(te)s les jour(s)**. Procédez aux mises à jour logicielles pendant les heures creuses ou lorsque le trafic réseau est faible.

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

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

Analyse à la demande et ses vues

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 e-mails ou des boîtes aux lettres spécifiques.

MSME 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.

Vous pouvez planifier des analyses régulières quand les activités de serveur sont relativement peu soutenues et que les analyses ne perturbent pas votre travail.

Cette fonctionnalité est uniquement disponible sur un serveur Exchange doté du rôle serveur de boîte aux lettres. Il est impossible de planifier une analyse à la demande sur un serveur Exchange disposant uniquement du rôle serveur de transport Edge ou serveur de transport Hub.

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 Exchange 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 Exchange ne sont pas infectées et que les anciens e-mails sont également analysés par les signatures antivirus les plus récentes. Les administrateurs doivent programmer une telle opération en tenant compte du nombre de serveurs Exchange, de bases de données et du flux d'e-mails. L'objectif doit être de mener à terme cette tâche avant les heures d'ouverture.

Avantages de l'analyse à la demande

Il peut s'avérer souhaitable d'effectuer une analyse à la demande pour un certain nombre de raisons. Par exemple :

- Pour vérifier un ou plusieurs fichiers téléchargés ou publiés
- Pour vérifier que les messages stockés sur le serveur Microsoft Exchange Server ne sont pas infectés, après la mise à jour des fichiers DAT, afin de détecter d'éventuels nouveaux virus
- Pour détecter et nettoyer un virus et vous assurer que l'ordinateur est complètement désinfecté

Affichage des tâches d'analyse à la demande

Affichez une liste des tâches d'analyse à la demande configurées pour MSME.

Procédure

- Cliquez sur **Tableau de bord** | **Analyses à la demande**. La page **Analyses à la demande** s'affiche avec les taches d'analyse à la demande configurées.

  Par défaut, une tâche d'analyse à la demande planifiée nommée **Analyse par défaut** est créée lors de l'installation de MSME.

  A la page **Analyses à la demande**, vous pouvez utiliser les options suivantes :

Tableau 2-3 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 : **Inactif**, **En cours d'exécution**, **Arrêtée** ou **Terminée**.
Dernière exécution	Indique les date et heure auxquelles la tâche d'analyse à la demande a été exécutée pour la dernière fois.
Exécution suivante	Indique les date et heure auxquelles la prochaine exécution de la tâche d'analyse à la demande est planifiée.
Action	Affiche les options ci-dessous pour toutes les tâches d'analyse à la demande disponibles : • **Modifier** • **Supprimer** • **Exécuter maintenant** • **Afficher le statut** L'option **Arrêter** s'affiche uniquement si une tâche d'analyse à la demande est en cours d'exécution.
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	Lance immédiatement la tâche d'analyse à la demande sélectionnée. L'option Exécuter maintenant est applicable uniquement après la création et l'application d'une tâche d'analyse à la demande non planifiée.
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 : • **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. L'option **Afficher le statut** est uniquement disponible après le démarrage d'une tâche d'analyse à la demande.
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.

Vous venez d'afficher toutes les tâches de rapport d'analyse à la demande disponibles configurées pour MSME.

Créer 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 boîtes aux lettres et ce, à des intervalles de temps pratiques.

Avant de commencer

Assurez-vous de ne pas supprimer de l'annuaire Active Directory l'utilisateur **MSMEODuser** créé au cours de l'installation du produit. L'exécution d'analyses à la demande des boîtes aux lettres requiert la présence de cet utilisateur.

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 **Choisir à quel moment effectuer l'analyse** s'affiche.

3 Dans 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 la tâche d'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 `2` 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 lorsqu'elle dépasse la durée d'exécution spécifiée en heures.

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 toutes les boîtes aux lettres d'Exchange Server.
- **Analyser les dossiers sélectionnés** : sélectionnez cette option pour analyser des boîtes aux lettres spécifiques au sein d'Exchange Server.
- **Analyser tous les dossiers sauf ceux sélectionnés** : sélectionnez cette option pour analyser toutes les boîtes aux lettres sauf celles qui ont été ajoutées à la liste **Dossiers à analyser**.

Dans Microsoft Exchange 2013 et 2016, le dossier public apparaît dans la boîte aux lettres et l'analyse à la demande est toujours récursive pour les dossiers publics. Dans Microsoft Exchange 2010, vous pouvez sélectionner un dossier public au niveau du dossier ou du sous-dossier pour exécuter l'analyse à la demande récursive.

5 Cliquez sur **Suivant**. La page **Configurer les paramètres d'analyse** s'affiche.

6 Dans la liste déroulante **Stratégie à utiliser**, sélectionnez l'option de stratégie répondant à vos exigences d'analyse.

Stratégie	Description
Par défaut	Paramètres par défaut applicables à tous les analyseurs et filtres à l'exception des analyseurs suivants : • **Analyseur de conformité et DLP** • **Filtrage de fichiers**
Rechercher les virus	Paramètres et filtres antivirus. Ces stratégies constituent un moyen facile de vérifier le contenu viral des bases de données.
Supprimer les virus	Paramètres et filtres antivirus. Ces stratégies constituent un moyen facile de supprimer le contenu viral des bases de données.
Rechercher le contenu non conforme	Paramètres d'analyse du contenu. Ces stratégies sont utiles si vous voulez observer l'effet de règles d'analyse de contenu que vous venez de créer ou d'affecter.
Supprimer le contenu non conforme	Paramètres d'analyse du contenu. Ces stratégies sont utiles si vous voulez observer l'effet de règles d'analyse de contenu que vous venez de créer ou d'affecter, et supprimer le contenu non conforme.
Analyse complète	Paramètres applicables à tous les analyseurs et filtres. Ces stratégies sont généralement adoptées pour une analyse exécutée à intervalle régulier.

Les paramètres et actions à appliquer sont indiqués dans les stratégies à la demande figurant sous **Gestionnaire de stratégies**.

7 Sélectionnez les options **Analyse avec reprise** et **Redémarrer à compter du dernier élément** pour exécuter la tâche d'analyse à la demande dans plusieurs sessions sur la base de données de boîte aux lettres.

Parfois, vous aurez peut-être besoin d'exécuter une tâche d'analyse à la demande pour toutes les boîtes aux lettres. L'analyse de toutes les boîtes aux lettres en une seule session peut durer plus longtemps, ce qui peut affecter la productivité du système. Au lieu d'analyser toutes les boîtes aux lettres en une seule session, vous pouvez planifier l'analyse sur plusieurs sessions.

8 Dans Exchange Server, vous avez désormais la possibilité d'effectuer une tâche d'analyse à la demande granulaire. Vous pouvez affiner l'analyse à l'aide des champs suivants :

- Objet
- De

- A
- ID du message
- Destinataires
- Plage de dates
- Taille de l'e-mail
- Pièces jointes
- Eléments non lus

L'exécution d'une analyse à la demande granulaire permet d'économiser du temps et d'obtenir des résultats d'analyse spécifiques.

9 Cliquez sur **Suivant**. La page **Entrer un nom pour l'analyse** s'affiche.

10 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`.

11 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 de statut

Un rapport de statut est un rapport planifié envoyé à un administrateur à un moment donné. Le rapport contient des statistiques de détection couvrant la période donnée.

La fonctionnalité **Rapports de statut** vous permet d'automatiser la tâche de requête régulière de statistiques. Vous pouvez planifier une tâche périodique de collecte de statistiques simples (le nombre de détections à une date donnée, par exemple) et envoyer un e-mail à l'administrateur Exchange ou à une liste de distribution.

Ces rapports vous aident à identifier les serveurs Exchange auxquels les menaces les plus nombreuses sont destinées, ce qui vous permet ensuite d'élaborer des mécanismes de réduction des menaces.

Vous pouvez choisir l'heure, l'adresse e-mail du destinataire ou la liste de distribution à laquelle envoyer le rapport, ainsi que l'objet de l'e-mail. Les rapports de statut sont envoyés au destinataire au format HTML ou CSV.

Selon la configuration, l'e-mail du rapport de statut contient des informations statistiques sur les éléments détectés tels que les virus, le spam, le phishing (hameçonnage), la réputation de l'adresse IP, les programmes potentiellement indésirables (PUP), les types de fichier interdits, le contenu indésirable, la conformité et la prévention des fuites de données (DLP), les e-mails non infectés et le nombre total d'e-mails analysés. Pour plus d'informations sur la planification d'un rapport de statut, consultez la section *Planification d'un nouveau rapport de statut*.

Une fois que vous avez installé MSME, les rapports de statut nécessitent un délai minimal de 24 heures avant de pouvoir remplir les statistiques dans l'e-mail de notification.

Affichage des tâches de rapport de statut

Affichez une liste des tâches de rapport d'état configurées pour MSME.

Procédure

- Cliquez sur **Tableau de bord** | **Rapports d'état**. La page **Rapports d'état** s'affiche, présentant une liste des tâches de rapport de statut configurées.

  A la page **Rapports de statut**, vous pouvez utiliser les options suivantes :

Tableau 2-4 Définition des options

Option	Définition
Nom	Indique le nom de la tâche de rapport.
Etat	Indique le statut de la tâche de rapport : **Inactif**, **En cours d'exécution**, **Arrêté**, ou **Terminée**.
Dernière exécution	Indique les date et heure auxquelles la tâche de rapport a été exécutée pour la dernière fois.
Prochaine exécution	Indique les date et heure auxquelles la prochaine exécution de la tâche de rapport est planifiée.
Action	Affiche la liste des options suivantes pour toutes les tâches de rapport disponibles : • **Modifier** • **Supprimer** • **Exécuter maintenant** • **Afficher le statut** L'option **Arrêter** s'affiche uniquement si une tâche de rapport est en cours d'exécution.
Modifier	Cliquez sur **Modifier** pour modifier les paramètres d'une tâche d'analyse à la demande.
Supprimer	Supprime la tâche de rapport sélectionnée.
Exécuter maintenant	Démarre immédiatement la tâche de rapport sélectionnée.
Afficher le statut	Affiche le statut d'une tâche de rapport. La page **Statut de la tâche** contient l'onglet suivant : • **Général** : présente des informations complémentaires sur la tâche de rapport telles que les heures de début et de fin, l'heure d'exécution de la tâche, l'action actuelle et la progression de la tâche. L'option **Afficher le statut** est uniquement disponible après le démarrage d'une tâche de rapport.
Actualiser	Actualise la page en y présentant les informations les plus récentes sur le rapport.
Nouveau rapport	Permet de planifier une nouvelle tâche de rapport d'état.

Vous venez d'afficher toutes les tâches de rapport d'état disponibles configurées pour MSME.

Planification d'un nouveau rapport de statut

Planifiez une nouvelle tâche de rapport de statut destinée à envoyer les statistiques de détection à une adresse e-mail précise ou à une liste de distribution, selon un intervalle qui vous convient.

Procédure

1 Cliquez sur **Tableau de bord** | **Rapports de statut**. L'écran **Rapports de statut** s'affiche.

2 Cliquez sur **Nouveau rapport**. La page **Rapport** s'affiche.

3 Sous l'onglet **Quand générer un rapport**, spécifiez le moment auquel vous souhaitez exécuter la tâche de rapport de statut. 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 rapport de statut ou pour désactiver la planification relative à une tâche existante de ce type.
- **Une fois** : spécifiez les date et heure auxquelles vous souhaitez planifier une tâche unique de rapport de statut.
- **Heures** : sélectionnez cette option pour planifier la tâche en fonction des heures, si vous devez exécuter la tâche de rapport de statut 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 de rapport remplissant les conditions suivantes :
  - la tâche de rapport de statut doit débuter à 14 h 30 exactement ;
  - la tâche de rapport de statut 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 de rapport de statut en fonction du nombre d'exécutions hebdomadaires souhaité. Par exemple, si la tâche 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 de rapport de statut en fonction du nombre d'exécutions mensuelles souhaité. Par exemple, si la tâche doit avoir lieu toutes les deux semaines, spécifiez `2` sous **semaine(s)**, puis sélectionnez les jours et l'heure auxquels la tâche doit démarrer.
- **Mois** : sélectionnez cette option pour planifier la tâche de rapport de statut en fonction du nombre d'exécutions annuelles souhaité. Par exemple, si la tâche 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 de rapport de statut si elle dépasse les heures d'exécution spécifiées.

4 Cliquez sur **Suivant**. La page **Paramètres du rapport** s'affiche. Les options disponibles sont les suivantes :

Tableau 2-5 Définition des options

Option	Définition
E-mail du destinataire	Indique l'adresse e-mail du destinataire ou l'adresse SMTP de la liste de distribution. Dans la plupart des cas, il s'agit de l'adresse e-mail de l'administrateur Exchange. Par défaut, l'adresse e-mail définie sous **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Général** | **E-mail de l'administrateur** est utilisée comme adresse e-mail du destinataire.
Ligne d'objet du rapport	Permet de spécifier une ligne d'objet évocatrice pour l'e-mail. Par exemple, si vous souhaitez générer un rapport de statut quotidien au format HTML, spécifiez `Rapport de statut quotidien MSME (HTML).`

Tableau 2-5 Définition des options *(suite)*

Option	Définition
Nombre de lignes	Indique le nombre de lignes (n) à afficher dans l'e-mail de rapport de statut. Chaque ligne du rapport de statut indique le nombre total de détections pour un jour particulier. Le rapport contient le nombre de détections pour les (n) derniers jours, sans compter le jour de déclenchement du rapport de statut. Par exemple : si vous précisez `1`, le rapport de statut contient une seule ligne qui affiche les détections de la veille. La valeur maximale admise est 365.
Type de rapport	Indique le format du rapport de statut envoyé au destinataire. Les options disponibles sont les suivantes : • **CSV** : permet d'envoyer le rapport de statut au destinataire au format texte séparé par des virgules, sous la forme d'une pièce jointe dotée de l'extension `.csv`. • **HTML** : permet d'envoyer le rapport de statut au destinataire au format HTML, sous la forme d'une pièce jointe dotée de l'extension .html ou directement dans le corps de l'e-mail.

5 Cliquez sur **Suivant**. La page **Entrez un nom de tâche** s'affiche.

6 Spécifiez un nom évocateur pour la tâche de rapport de statut, en fonction de la planification et du format sélectionnés aux pages précédentes. Par exemple, si vous créez une tâche de rapport de statut hebdomadaire destinée à présenter les statistiques de détection de la semaine au format HTML, donnez à la tâche un nom du genre `Rapport de statut hebdomadaire (HTML)`.

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

En suivant ces étapes, vous êtes parvenu au terme de la création d'une tâche de rapport de statut.

Notifications par e-mail relatives aux rapports de statut

Selon le rapport de statut planifié, le destinataire reçoit un e-mail présentant les statistiques sur tous les e-mails analysés et détectés par MSME pour la durée définie.

Suivant la configuration du rapport de statut, l'e-mail contient des informations statistiques sur les éléments détectés, le nombre total d'e-mails non infectés et le nombre total d'e-mails analysés ce jour-là.

Tableau 2-6 Définition des options

Option	Définition
De	Affiche l'adresse e-mail que vous avez spécifiée sous **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Général** | **E-mail de l'expéditeur**.
A	Affiche l'adresse e-mail du destinataire visé que vous avez spécifiée sous **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Général** | **E-mail de l'administrateur**.
Objet	Affiche l'objet de la notification par e-mail sur le rapport de statut que vous avez spécifié sous **Tableau de bord** | **Rapports d'état** | **Paramètres du rapport** | **Ligne d'objet du rapport**.
Statistiques d'analyse pour le serveur	Affiche le **Nom de l'ordinateur** sur lequel MSME est installé.
Date	Affiche la date au format MM/JJ/AAAA.
Détections	Affiche les statistiques de détection des catégories **Virus**, **Spam**, **Phishing**, **Réputation de l'adresse IP**, **Programme potentiellement indésirable**, **Types de fichiers interdits**, **Contenu indésirable**, et **Conformité et DLP** dans le corps du message. Les statistiques **Spam**, **Hameçonnage** et **Réputation de l'adresse IP** sont disponibles uniquement si le module complémentaire McAfee Anti-Spam est installé.

Tableau 2-6 Définition des options *(suite)*

Option	Définition
Nettoyer	Affiche le nombre total d'e-mails non infectés qui ont été détectés par MSME comme non infectés et qui ne constituaient pas une menace. Par exemple, même les e-mails de rapport d'état envoyés à l'administrateur sont comptés comme e-mails non infectés dans les statistiques.
Nombre total d'éléments analysés	Affiche le nombre total d'e-mails analysés par MSME pour la journée.

Les e-mails de rapport d'état sont bloqués si vous avez attribué la valeur **Seuil de réputation des adresses IP** à l'option **Adresse IP approuvée (score inférieur à 0)** ou **Adresse IP neutre (score supérieur ou égal à 0)** via le menu **Paramètres et diagnostics** | **Anti-Spam** | **Réputation des adresses IP McAfee GTI**.

Rapports de configuration

Un rapport de configuration désigne un rapport planifié envoyé à un administrateur à un moment donné. Ce rapport contient les informations produit, paramètres de stratégie et données système concernant MSME.

La fonctionnalité **Rapports de configuration** permet d'automatiser la tâche d'affichage périodique de la synthèse des configurations produit.

Cette fonctionnalité s'avère pratique dans les organisations comptant plusieurs administrateurs qui souhaitent assurer un suivi des paramètres de configuration MSME. Celle-ci est également utile lorsque vous disposez de plusieurs installations de MSME managées par ePolicy Orchestrator et que vous souhaitez localiser la configuration de produit.

Vous pouvez choisir l'heure, l'adresse e-mail du destinataire ou la liste de distribution auxquelles envoyer le rapport, ainsi que l'objet de l'e-mail.

Selon la configuration définie, le rapport de configuration contient des informations relatives au produit et au système de ce type : informations sur le serveur, informations sur la version du produit, statut et type de la licence, informations sur les HotFix, informations sur la journalisation de débogage, paramètres de l'analyseur à l'accès, paramètres de stratégie à l'accès et paramètres de stratégie de passerelle. Pour plus d'informations sur la planification d'un rapport de configuration, consultez la section *Planification d'un nouveau rapport de configuration*.

Affichage des tâches de rapport de configuration

Affichez une liste des tâches de rapport de configuration définies pour MSME.

Procédure

- Cliquez sur **Tableau de bord** | **Rapports de configuration**. La page **Rapports de configuration** s'affiche, présentant une liste des tâches de rapport de configuration définies.

  A la page **Rapports de configuration**, vous pouvez utiliser les options suivantes :

  Tableau 2-7 Définition des options

Option	Définition
Nom	Indique le nom de la tâche de rapport.
Etat	Indique le statut de la tâche de rapport : **Inactif**, **En cours d'exécution**, **Arrêté**, ou **Terminée**.
Dernière exécution	Indique les date et heure auxquelles la tâche de rapport a été exécutée pour la dernière fois.

Tableau 2-7 Définition des options *(suite)*

Option	Définition
Prochaine exécution	Indique les date et heure auxquelles la prochaine exécution de la tâche de rapport est planifiée.
Action	Affiche la liste des options suivantes pour toutes les tâches de rapport disponibles : • **Modifier** • **Supprimer** • **Exécuter maintenant** • **Afficher le statut** L'option **Arrêter** s'affiche uniquement si une tâche de rapport est en cours d'exécution.
Modifier	Cliquez sur **Modifier** pour modifier les paramètres d'une tâche d'analyse à la demande.
Supprimer	Supprime la tâche de rapport sélectionnée.
Exécuter maintenant	Démarre immédiatement la tâche de rapport sélectionnée.
Afficher le statut	Affiche le statut d'une tâche de rapport. La page **Statut de la tâche** contient l'onglet suivant : • **Général** : présente des informations complémentaires sur la tâche de rapport telles que les heures de début et de fin, l'heure d'exécution de la tâche, l'action actuelle et la progression de la tâche. L'option **Afficher le statut** est uniquement disponible après le démarrage d'une tâche de rapport.
Actualiser	Actualise la page en y présentant les informations les plus récentes sur le rapport.
Nouveau rapport	Permet de planifier une nouvelle tâche de configuration de statut.

Vous venez d'afficher toutes les tâches de rapport de configuration disponibles définies pour MSME.

Planification d'un nouveau rapport de configuration

Planifiez une nouvelle tâche de rapport de configuration destinée à envoyer la configuration du produit et les informations sur le système à une adresse e-mail précise ou à une liste de distribution, selon un intervalle qui vous convient.

Procédure

1 Cliquez sur **Tableau de bord** | **Rapports de configuration**. La page **Rapports de configuration** s'affiche.

2 Cliquez sur **Nouveau rapport**. La page **Rapport** s'affiche.

3 Sous l'onglet **Quand générer un rapport**, spécifiez le moment auquel vous souhaitez exécuter la tâche de rapport de configuration. 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 rapport de configuration ou pour désactiver la planification relative à une tâche existante de ce type.
- **Une fois** : spécifiez les date et heure auxquelles vous souhaitez planifier une tâche unique de rapport de configuration.

- **Heures** : sélectionnez cette option pour planifier la tâche en fonction des heures, si vous devez exécuter la tâche de rapport de configuration 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 de rapport remplissant les conditions suivantes :
  - la tâche de rapport de configuration doit débuter à 14 h 30 exactement ;
  - la tâche de rapport de configuration 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 de rapport de configuration en fonction du nombre d'exécutions hebdomadaires souhaité. Par exemple, si la tâche 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 de rapport de configuration en fonction du nombre d'exécutions mensuelles souhaité. Par exemple, si la tâche doit avoir lieu toutes les deux semaines, spécifiez `2` sous **semaine(s)**, puis sélectionnez les jours et l'heure auxquels la tâche doit démarrer.
- **Mois** : sélectionnez cette option pour planifier la tâche de rapport de configuration en fonction du nombre d'exécutions annuelles souhaité. Par exemple, si la tâche 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 de rapport de configuration si elle dépasse les heures d'exécution spécifiées.

4 Cliquez sur **Suivant**. La page **Paramètres du rapport** s'affiche. Les options disponibles sont les suivantes :

Tableau 2-8 Définition des options

Option	Définition
E-mail du destinataire	Indique l'adresse e-mail du destinataire ou l'adresse SMTP de la liste de distribution. Dans la plupart des cas, il s'agit de l'adresse e-mail de l'administrateur Exchange. Par défaut, l'adresse e-mail définie sous **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Général** | **E-mail de l'administrateur** est utilisée comme adresse e-mail du destinataire.
Ligne d'objet du rapport	Permet de spécifier une ligne d'objet évocatrice pour l'e-mail. Par exemple, si vous souhaitez générer un rapport de configuration hebdomadaire, indiquez `Rapport de configuration hebdomadaire MSME`.

5 Cliquez sur **Suivant**. La La page **Entrez un nom de tâche** s'affiche.

6 Spécifiez un nom évocateur pour la tâche de rapport de configuration, en fonction de la planification et du format sélectionnés aux pages précédentes. Par exemple, si vous créez une tâche mensuelle comprenant des informations sur le produit et le système le premier lundi de chaque mois, donnez à la tâche un nom du genre `Rapport de configuration mensuel (premier lundi du mois)`.

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

En suivant ces étapes, vous êtes parvenu au terme de la création d'une tâche de rapport de configuration.

Notifications par e-mail relatives aux rapports de configuration

Selon le rapport de configuration planifié, le destinataire reçoit un e-mail contenant les informations produit, paramètres de stratégie et données système concernant MSME pour la période indiquée.

Tableau 2-9 Définition des options

Option	Définition
Infos sur le serveur	Affiche des informations sur le serveur telles que le nom de l'ordinateur, l'adresse IP et la version d'Exchange.
Infos sur la version	Affiche des informations concernant MSME telles que la version du produit, la version et la date des fichiers DAT, la version du moteur, et des informations sur les règles antispam et le moteur (le cas échéant).
Statut de licence pour	Affiche des informations relatives à la licence du produit telles que le type de licence de MSME et du composant de module complémentaire Anti-Spam.
Informations produit	Affiche des informations produit supplémentaires, notamment la présence de tout Service Pack ou HotFix.
Consignation du débogage	Affiche des informations de **Consignation de débogage** telles que le niveau de détail, la taille maximale du fichier journal et l'emplacement du fichier.
Paramètres à l'accès	Affiche la configuration actuelle des **Paramètres à l'accès** (ceux qui sont activés et ceux qui ne le sont pas).
Stratégies d'analyse à l'accès	Affiche les analyseurs et filtres de base activés pour la **Stratégie principale A l'accès**.
Stratégies de passerelles	Affiche le statut actuel de l'analyseur antispam et antiphishing pour la **Stratégie principale | Passerelle**. Cette option s'applique uniquement lorsque le composant de module complémentaire McAfee Anti-Spam est installé.

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 d'un **Graphique à secteurs**.

Ces rapports, ainsi que le rapport de statut, vous aideront, vous et votre organisation, à identifier les serveurs confrontés aux menaces les plus importantes et à élaborer des plans de réduction.

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** : comprend les filtres de recherche limitée 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 du rapport graphique 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

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 **Filtrer**, 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.
- **Classement des 10 premières détections de spams** : répertorie les 10 principaux e-mails de spam détectés en les classant d'après leur nombre d'occurrences.
- **Classement des 10 premiers destinataires de spams** : répertorie les 10 principaux destinataires d'e-mails de spam en les classant d'après le nombre total d'occurrences détectées.
- **Classement des 10 premières détections d'hameçonnage** : répertorie les 10 principaux e-mails de phishing (hameçonnage) détectés en les classant d'après leur nombre d'occurrences.
- **10 principales adresses IP bloquées** : répertorie les 10 principales adresses IP bloquées en les classant d'après le nombre d'e-mails retournés.
- **10 principaux programmes indésirables** répertorie les 10 principaux programmes potentiellement indésirables détectés pouvant constituer des menaces.
- **10 premières détections TIE** : affiche les 10 principales menaces potentielles détectées par TIE.
- **10 premières détections d'usurpation** : affiche les 10 principaux e-mails d'usurpation détectés.
- **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 principales URL bloquées** — Répertorie les 10 principales URL détectées pouvant constituer des menaces.
- **10 premières détections** : répertorie les 10 principales détections en les classant d'après leur nombre d'occurrences. Ce graphique englobe toutes les catégories : virus, détections de spam, destinataires de messages de spam, détections de messages de phishing, adresses IP bloquées, programmes indésirables, conformité et prévention des fuites de données (DLP), les URL malveillantes et les fichiers infectés répertoriés précédemment.

5 Cliquez sur **Recherche**. Les résultats de la recherche apparaissent dans le volet **Afficher les résultats**.

Sous **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**.

Utilisation de filtres de recherche avancés

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

Procédure

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 2-10 Filtres principaux

Filtre	Description
Objet	Permet d'effectuer la recherche d'après la ligne d'objet d'un e-mail.
Destinataires	Permet d'effectuer la recherche d'après l'adresse e-mail du destinataire.
Raison	Permet d'effectuer la recherche à l'aide du déclencheur de détection ou de la raison de la mise en quarantaine de l'élément. Lorsque vous sélectionnez le filtre **Raison**, les filtres secondaires sont activés, ce qui vous permet d'affiner la recherche. Par exemple, pour rechercher tous les éléments qui ont été mis en quarantaine suite au déclenchement de la règle **Taille de l'e-mail** 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 détection	Permet d'effectuer la recherche selon le nom d'un élément détecté.
Pertinence des spams	Permet de baser la recherche sur le score de spam. Par exemple, pour rechercher tous les éléments qui ont été mis en quarantaine et dont le **Pertinence des spams** est défini sur 3.

L'option **Score de spam** indique le nombre de messages de spam potentiels contenus dans un e-mail. Le moteur applique des règles antispam à chaque e-mail analysé. Un score est associé à chaque règle. Afin d'évaluer le risque de présence d'un spam dans un e-mail, ces scores sont additionnés en vue d'obtenir un score de spam global pour cet e-mail. Plus le score de spam global est élevé, plus il est probable qu'il s'agisse d'un spam. Le score de spam peut osciller entre 0 et 100. A leur entrée, les messages se voient attribuer un score de spam de zéro. Ce score augmente à chaque violation d'un filtre par les messages.

Un filtre secondaire est disponible uniquement pour le filtre **Raison**. Si vous préférez ne pas préciser de filtre secondaire, assurez-vous que le champ est vide afin que toutes les détections soient interrogées.

Tableau 2-11 Filtres secondaires

Filtre	Description
Antivirus	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un virus potentiel dans le message.
Conformité et DLP	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu interdit dans le message, des mots inappropriés, par exemple.
Filtre de fichiers	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un fichier interdit dans l'e-mail.
Antispam	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un spam, des e-mails en chaîne, par exemple.
Réputation de l'adresse IP	Permet de rechercher les éléments qui ont été mis en quarantaine suite au dépassement du seuil défini par la réputation de l'URL.
Crypté ou corrompu	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu chiffré ou corrompu dans l'e-mail.
Programme potentiellement indésirable	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un programme potentiellement indésirable dans l'e-mail.
Phishing	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu de phishing dans l'e-mail.

Tableau 2-11 Filtres secondaires *(suite)*

Filtre	Description
Programme de compression	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection de programmes de compression (programmes de petite taille, fichiers exécutables compressés ou code chiffré) dans l'e-mail.
Taille de l'e-mail	Permet de rechercher les éléments qui ont été mis en quarantaine suite au dépassement de la limite maximale définie pour la taille d'e-mail.
Crypté	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu chiffré dans l'e-mail.
Signé	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu signé dans l'e-mail.
Corrompu	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu corrompu dans l'e-mail.
Déni de service	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la présence d'une menace par déni de service, en vue de la récupération de l'ensemble des e-mails mis en quarantaine dans une telle situation, par exemple.
Contenu protégé	Permet de rechercher les éléments qui ont été mis en quarantaine lorsqu'un contenu protégé a été détecté, sans toutefois avoir été examiné.
Protégé par mot de passe	Permet de rechercher les éléments qui ont été mis en quarantaine lorsqu'un contenu protégé par mot de passe a été détecté, sans toutefois avoir été examiné.
MIME bloqué	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu MIME (Multipurpose Internet Mail Extension) bloqué dans l'e-mail.
Réputation de l'URL	Permet de rechercher les éléments qui ont été mis en quarantaine suite au dépassement du seuil défini pour la réputation de l'URL.
Réputation TIE	Permet de rechercher les éléments qui ont été mis en quarantaine suite au dépassement du seuil défini pour la réputation TIE.
Erreur logicielle SPF	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu d'usurpation dans l'e-mail.
Erreur matérielle SPF	Permet de rechercher les éléments qui ont été mis en quarantaine suite à la détection d'un contenu d'usurpation dans l'e-mail.

Pour plus d'informations sur les filtres de recherche, consultez la section *Filtres de recherche*.

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 les valeurs **Date**, **Mois**, **Année**, **Heure** et **Minutes** à partir des 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 2-12 Options d'objet de la requête

Filtre	Description
Destinataires	Permet d'effectuer la recherche d'après l'adresse e-mail du destinataire.
Expéditeur	Permet d'effectuer la recherche d'après l'adresse e-mail de l'expéditeur.
Nom de fichier	Permet d'effectuer la recherche d'après le nom d'un fichier mis en quarantaine.

Tableau 2-12 Options d'objet de la requête *(suite)*

Filtre	Description
Nom de la détection	Permet d'effectuer la recherche d'après le nom d'un élément détecté.
Objet	Permet d'effectuer la recherche d'après la ligne d'objet d'un e-mail.
Raison	Permet d'effectuer la recherche d'après le déclencheur de détection ou la raison de la mise en quarantaine de l'élément.
Nom de la règle	Permet d'effectuer la recherche d'après le nom de la règle ayant déclenché la détection.
Nom de la stratégie	Permet d'effectuer la recherche d'après le nom de la règle ayant déclenché la détection.

a Sous **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 figurent 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**.

3 Eléments détectés

Affichez des informations relatives à tous les e-mails contenant des menaces potentielles qui sont détectés et mis en quarantaine par MSME. 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.

A partir de l'interface utilisateur du produit, cliquez sur **Eléments détectés** pour afficher les éléments mis en quarantaine en fonction de la catégorie de détection. Les catégories de détection sont les suivantes :

- **Spam**
- **Réputation de l'adresse IP**
- **Phishing**
- **Virus**
- **Détections TIE et ATD**
- **E-mails falsifiés**
- **Programmes potentiellement indésirables**
- **Contenu indésirable**
- **Types de fichiers et messages interdits**
- **Conformité et DLP**
- **Réputation de l'URL de courrier**
- **Tous les éléments**

Les options **Spam**, **Hameçonnage**, **Filtre SPF** et **Réputation de l'adresse IP** sont disponibles uniquement si vous avez installé le module complémentaire McAfee Anti-Spam.

Sommaire

Gestion des données mises en quarantaine

Selon les exigences de l'entreprise, vous opterez soit pour la base de données locale soit pour un serveur de gestion de quarantaine dédié appelé McAfee Quarantine Manager, qui se chargera de mettre en quarantaine les éléments détectés.

Par défaut, les éléments détectés sont mis en quarantaine localement dans une base de données PostgreSQL installée par MSME.

Configuration de l'emplacement de mise en quarantaine

Selon les paramètres de configuration définis pour l'option **Eléments détectés**, vous pouvez choisir de mettre en quarantaine les éléments détectés dans la base de données locale ou d'utiliser le logiciel Quarantine Management de McAfee, largement connu sous l'appellation McAfee Quarantine Manager pour mettre en quarantaine les éléments détectés sur un serveur distinct.

Pour les systèmes managés, si vous sélectionnez le serveur MQM pour mettre en quarantaine les éléments détectés, assurez-vous que la configuration est mise en œuvre uniquement sur les systèmes que vous avez choisis. Dans le cas contraire, la configuration est appliquée à l'ensemble des serveurs MSME dans l'**Arborescence des systèmes**.

A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Eléments détectés**, puis sélectionnez :

- **McAfee Quarantine Manager** : permet de mettre en quarantaine les éléments détectés sur le serveur MQM.
- **Base de données locale** : permet de mettre en quarantaine les éléments détectés sur le serveur MSME, dans le chemin d'accès indiqué.

Base de données locale et McAfee Quarantine Manager — Cas d'utilisation

Ce tableau vous aide à comprendre les situations où il est plus indiqué d'utiliser la base de données locale pour la gestion de quarantaine et ceux où McAfee Quarantine Manager est préférable :

Utilisation de la base de données locale	Utilisation de McAfee Quarantine Manager...
Pour gérer les éléments mis en quarantaine d'une installation MSME.	Pour gérer les éléments mis en quarantaine pour plusieurs installations de MSME ou pour l'un des produits MSME configurés dans votre organisation : • McAfee Security for Microsoft Exchange • McAfee Email and WebSecurity Appliance • McAfee Security for Lotus Domino (Windows) Vous pouvez télécharger et installer McAfee Quarantine Manager gratuitement si vous avez acquis l'un des produits indiqués ci-dessus.
Pour mettre des éléments en quarantaine à l'aide de la base de données PostgreSQL	Pour mettre des éléments en quarantaine à l'aide de la base de données MySQL ou Microsoft SQL Server

Pour plus d'informations sur le logiciel McAfee Quarantine Manager et sur ses fonctionnalités, consultez la documentation produit correspondante.

Types de détection

Les éléments détectés sont des e-mails identifiés par MSME comme des menaces potentielles. Ils peuvent prendre la forme d'un virus, d'un message de spam, d'un message de phishing, d'un contenu non conforme, une URL ou de types de fichier interdits.

Les types de détection disponibles dans MSME sont les suivants :

Types de détection	Description
Spam	Message électronique indésirable, généralement un e-mail à diffusion massive non sollicité. Le plus souvent, il s'agit d'un message envoyé à un grand nombre de destinataires qui n'ont pas demandé à le recevoir. Le spam peut toucher différents systèmes : la messagerie électronique, la messagerie instantanée, les groupes de discussion d'actualités Usenet, les moteurs de recherche sur le web, les blogs et la messagerie de téléphonie mobile. Le spam comprend des publicités légitimes, des publicités trompeuses et des messages de phishing destinés à amener les destinataires peu méfiants à communiquer leurs informations personnelles et financières. Un e-mail n'est pas considéré comme du spam si l'utilisateur a explicitement donné son consentement pour qu'il lui soit envoyé.
Réputation de l'adresse IP	Méthode de détection des messages reposant sur l'adresse IP du serveur d'envoi. McAfee collecte des données provenant de milliards d'adresses IP et de ports réseau, offrant plusieurs centaines de trillions de vues uniques, et calcule un score de réputation à partir du trafic réseau (incluant le port, la destination, le protocole et les demandes de connexion entrantes et sortantes). Ce score est connu sous l'appellation de **Score de réputation de l'adresse IP**. Il reflète la probabilité de menace que pose une connexion réseau donnée. MSME utilise ce score pour identifier une action en fonction d'une stratégie locale.
Phishing	Méthode consistant à obtenir frauduleusement des informations personnelles, telles que des mots de passe, des numéros de sécurité sociale et des numéros de carte de crédit en envoyant des e-mails semblant provenir de sources approuvées, telles que des banques ou des entreprises légitimes. En général, les e-mails de phishing demandent aux destinataires de cliquer sur le lien contenu dans l'e-mail pour vérifier ou mettre à jour des coordonnées ou des informations de carte de crédit. A l'instar du spam, les e-mails de phishing sont envoyés à un grand nombre d'adresses e-mail dans l'espoir qu'un destinataire les lira et divulguera ses informations personnelles.
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. Vous ne pouvez pas **Télécharger**, **Libérer**, **Transférer**, ou **Afficher** les éléments mis en quarantaine à partir de la catégorie de détection **Virus**.
Détections TIE et ATD	Outre DAT et McAfee GTI, vous pouvez maintenant utiliser les fonctionnalités de détection améliorée de McAfee Global Threat Intelligence et de McAfee Advanced Threat Defense.
E-mails falsifiés	L'usurpation d'e-mails est une escroquerie fréquente consistant à capter les utilisateurs en leur envoyant un e-mail avec une adresse d'expéditeur différente de celle indiquée. Les utilisateurs ouvrent alors l'e-mail et y répondent, croyant qu'il provient d'une source légitime.
Programmes potentiellement indésirables	Logiciels généralement légitimes (contrairement aux logiciels malveillants ou malware) qui peuvent altérer l'état de sécurité ou la position de confidentialité du système sur lequel ils sont installés. Ces logiciels incluent quelquefois (mais pas nécessairement) des logiciels espions (spyware), des logiciels publicitaires (adware), des enregistreurs de frappe, des craqueurs de mot de passe et des applications numéroteurs. Ils peuvent être téléchargés en même temps qu'un programme souhaité par l'utilisateur. Les utilisateurs soucieux de préserver la sécurité de leur système souhaitent parfois en savoir plus sur ces programmes et, dans certains cas, les supprimer.

Types de détection	Description
Contenu indésirable	Contenu qui déclenche une règle d'analyse de contenu. Il peut s'agir de termes offensants, injurieux, déplaisants, voire des informations confidentielles sur l'entreprise. Le type **Contenu non désirable** peut être classé selon les catégories suivantes : • **Programmes de compression** • **Contenu crypté** • **Contenu signé** • **Contenu corrompu** • **Déni de service** • **Contenu protégé** • **Fichiers protégés par mot de passe** • **Messages MIME incomplets**
Types de fichiers et messages interdits	Certains types de pièce jointe sont susceptibles d'être des virus. Le blocage des pièces jointes en fonction de leur extension de fichier offre à votre système de messagerie un niveau de sécurité supplémentaire. Les messages et les types de fichier interdits sont tous recherchés dans les e-mails internes et externes.
Conformité et DLP	Arrêtez la fuite de données confidentielles par e-mail. MSME offre une fonctionnalité d'analyse de contenu des e-mails 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. Favorisez la prévention des fuites de données en utilisant Data Loss Prevention (DLP), la solution de protection de messagerie 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.
Réputation de l'URL de courrier	Empêche la remise d'e-mails contenant des URL indésirables pouvant contenir des liens indésirables, des liens de phishing ou des logiciels malveillants.

Les options **Spam**, **Hameçonnage**, **Filtre SPF** et **Réputation de l'adresse IP** sont disponibles uniquement si vous avez installé le module complémentaire McAfee Anti-Spam.

Voir aussi

Tableau de comparaison des filtres de recherche, page 47
Options de recherche supplémentaires, page 49

Principaux filtres de recherche disponibles

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.

Les principaux filtres de recherche mis à disposition varient en fonction de la catégorie d'éléments détectés sélectionnée. 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 3-1 Eléments détectés — Principaux filtres de recherche

Filtre de recherche	Définition
Action entreprise	Permet de rechercher un élément en fonction de l'action entreprise associée. Les actions entreprises par MSME sont les suivantes : • **Nettoyer** • **Nettoyé** • **Supprimé** • **Message supprimé** • **Accès refusé** • **Consigné** • **Remplacé** • **Rejeté**
Moteur antispam	Permet de rechercher un élément en fonction du moteur antispam qui analyse les e-mails à la recherche de spam et d'attaques par phishing. Pour afficher le **Moteur antispam** actuellement utilisé, accédez à **Tableau de bord** | **Versions & Mises à jour** | **Informations de mise à jour** | **Moteur antispam** | **Version des règles**. Par exemple, la version du **Moteur antispam** est indiquée au format suivant : 9286
Règle antispam	Permet de rechercher un élément en fonction des règles antispam mises à jour toutes les deux ou trois minutes pour détecter les dernières campagnes de spam envoyées par les spammeurs. Pour afficher la **Règle antispam** actuellement utilisée, accédez à **Tableau de bord** | **Versions & Mises à jour** | **Informations de mise à jour** | **Moteur antispam** | **Version des règles**. Par exemple, la version d'une règle s'affiche au format suivant : core:4373:streams:840082:uri:1245250
Fichier DAT de l'antivirus	Permet de rechercher un élément en fonction de la version des fichiers DAT de l'antivirus qui comprend une signature distinctive. Pour afficher le **fichier DAT de l'antivirus** actuellement utilisé, accédez à **Tableau de bord** | **Versions & Mises à jour** | **Informations de mise à jour** | **Moteur antivirus** | **Version des fichiers DAT** | **Pilotes supplémentaires**. Par exemple, la version des fichiers DAT s'affiche au format suivant : 6860.0000
Moteur antivirus	Permet de rechercher un élément en fonction du moteur antivirus doté d'une séquence de caractères unique pour un contenu indésirable/virus. Pour afficher le **Moteur antivirus** actuellement utilisé, accédez à **Tableau de bord** | **Versions & Mises à jour** | **Informations de mise à jour** | **Moteur antivirus** | **Version des fichiers DAT** | **Pilotes supplémentaires**. Par exemple, la version du **Moteur antivirus** est indiquée au format suivant : 5400.1158
Phrases interdites	Permet de rechercher des éléments en fonction du contenu d'expressions interdites définies via l'option **Règles de conformité et DLP**, sous **Gestionnaire de stratégies** | **Ressource partagée** | **Dictionnaires de conformité et DLP**.
Nom de la détection	Permet de rechercher un élément détecté en fonction de son nom.
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 de fichiers**.
Dossier	Permet d'effectuer une recherche en fonction du dossier contenant les éléments mis en quarantaine (la boîte aux lettres d'un utilisateur, par exemple). Le dossier n'est pas disponible si l'e-mail est mis en quarantaine au niveau (du trafic) à l'accès.

Tableau 3-1 Eléments détectés — Principaux filtres de recherche *(suite)*

Filtre de recherche	Définition
Score de réputation de l'adresse IP	Permet de rechercher un élément en fonction de la valeur de l'option **Score de réputation de l'adresse IP** de l'expéditeur. Les éléments mis en quarantaine sont définis en fonction de l'option **Seuil de réputation des adresses IP** spécifiée sous **Paramètres et diagnostics** | **Antispam** | **Réputation des adresses IP McAfee GTI**. Ce filtre est uniquement disponible si le composant de module complémentaire McAfee Anti-Spam est installé.
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. Il peut s'agir d'analyseurs et de filtres comme **Antivirus**, **Antispam**, **Antihameçonnage**, **Conformité et DLP**, etc.
Raisons	Permet d'effectuer une recherche en fonction d'une ou de plusieurs règles déclenchées par un e-mail particulier. Utilisez cette option si un élément a déclenché plusieurs analyseurs ou filtres. Par exemple, si un e-mail de spam contient un virus, l'option **Raisons** indique **Antispam** et **Antivirus**.
Destinataires	Permet de rechercher un élément en fonction de l'adresse e-mail du destinataire.
Score de réputation	Permet d'effectuer une recherche en fonction du niveau d'authenticité de la source de l'e-mail, d'après les informations à jour disponibles. Les éléments mis en quarantaine sont définis en fonction de l'option **Seuil de réputation des messages** spécifiée sous **Paramètres et diagnostics** | **Antispam** | **Réputation des messages McAfee GTI**. Ce filtre est uniquement disponible si le module complémentaire McAfee Anti-Spam est installé.
Nom de la règle	Permet de rechercher un élément en fonction de la règle ayant déclenché un ou plusieurs analyseurs/filtres. La règle ayant déclenché l'analyseur ou le filtre est basée sur les **Actions** attribuées à chaque stratégie.
Analysé par	Permet de rechercher un élément en fonction du nom de l'analyseur l'ayant détecté.
Expéditeur	Permet de rechercher un élément en fonction de l'adresse e-mail de l'expéditeur.
Adresse IP de l'expéditeur	Permet de rechercher un élément en fonction de l'adresse IP du système de l'expéditeur. Les éléments mis en quarantaine sont définis en fonction de l'option **Seuil de réputation des adresses IP** spécifiée sous **Paramètres et diagnostics** | **Antispam** | **Réputation des adresses IP McAfee GTI**. Ce filtre est uniquement disponible si le module complémentaire McAfee Anti-Spam est installé.
Serveur	Permet de rechercher un élément en fonction du nom de l'ordinateur.
Pertinence des spams	Permet de rechercher un élément en fonction du score de spam. Il s'agit d'un nombre indiquant la quantité de spam potentiel contenue dans un e-mail. Le moteur applique des règles antispam à chaque e-mail analysé. Un score est associé à chaque règle. Afin d'évaluer le risque qu'un e-mail contienne du spam, ces scores sont additionnés en vue d'obtenir un score de spam global pour cet e-mail. Plus le score de spam global est élevé, plus il est probable qu'il s'agisse d'un message de spam. Ce filtre est disponible uniquement si le module complémentaire McAfee Anti-Spam est installé.

Tableau 3-1 Eléments détectés — Principaux filtres de recherche *(suite)*

Filtre de recherche	Définition
Etat	Permet de rechercher un élément en fonction de son état actif. Les états disponibles pour les éléments sont les suivants : • **Supprimé de l'apprentissage** : désigne les éléments pour lesquels aucune action n'est entreprise (éléments purgés, libérés, transférés ou supprimés, par exemple). L'état initial attribué à tous les éléments est **Supprimé de l'apprentissage**. • **Libéré** : désigne les éléments libérés de la base de données de quarantaine. • **Dans la file d'attente Quarantine Manager** : désigne les éléments figurant dans la file d'attente au sein de la base de données McAfee Quarantine Manager. • **Transféré** : désigne les éléments transférés aux destinataires attendus.
Objet	Permet de rechercher un élément d'après la ligne de l'objet de l'e-mail.
Tâche	Permet de rechercher un élément en fonction du nom de la tâche d'analyse, qui peut correspondre à une tâche d'analyse (VSAPI) à l'accès, à une tâche d'analyse (du trafic) à l'accès ou encore à une tâche d'analyse à la demande. La tâche d'analyse à l'accès figurant dans la section **Afficher les résultats** est basée sur les paramètres activés sous **Paramètres et diagnostics** | **Paramètres à l'accès**. Pour savoir si l'élément a été détecté suite à une tâche d'analyse à la demande, accédez à **Tableau de bord** | **Analyses à la demande**.
Numéro de ticket	Recherche un élément en fonction du numéro de ticket, lequel désigne un identificateur alphanumérique unique affecté à une détection spécifique et remis en tant que notification par e-mail. Il permet d'identifier la détection associée.
Score TIE	Permet de rechercher des éléments d'après leur score de réputation TIE.

Les principaux filtres de recherche applicables aux catégories de détection **Spam**, **Hameçonnage** et **Réputation de l'adresse IP** sont disponibles uniquement si le module complémentaire McAfee Anti-Spam est installé.

Voir aussi

Options de recherche supplémentaires, page 49

Tableau de comparaison des filtres de recherche

Ce graphique présente des informations sur les filtres de recherche disponibles selon la catégorie d'éléments détectés sélectionnée.

Les filtres de recherche disponibles dans MSME varient en fonction de la catégorie d'éléments détectés sélectionnée. Référez-vous à ce tableau en cas de doute sur les filtres de recherche disponibles pour telle ou telle catégorie d'éléments détectés.

En jetant un simple coup d'œil à ce tableau de comparaison, vous prendrez connaissance des filtres disponibles pour un type de détection donné.

Tableau 3-2 Tableau de comparaison — Filtres de recherche associés aux types de détection

Filtre	Spam	IP Réputation	Phishing	Virus	Potentiellement Indésirables Programmes	Indésirables Contenu	Interdit Types de fichiers et Messages	DLP et Conformité	E-mail URL Réputation
Action entreprise	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moteur antispam	✓		✓						

Tableau 3-2 Tableau de comparaison — Filtres de recherche associés aux types de détection *(suite)*

Filtre	Spam	IP Réputation	Phishing	Virus	Potentiellement Indésirables Programmes	Indésirables Contenu	Interdit Types de fichiers et Messages	DLP et Conformité	E-mail URL Réputation
Règle antispam	✓		✓						
Fichier DAT de l'antivirus				✓	✓				
Moteur antivirus				✓	✓				
Phrases interdites						✓		✓	✓
Nom de détection				✓	✓				
Nom de fichier				✓	✓	✓	✓	✓	✓
Dossier				✓	✓	✓	✓	✓	✓
Score de réputation de l'adresse IP		✓							
Nom de stratégie	✓		✓	✓	✓	✓	✓	✓	✓
Destinataires	✓		✓	✓	✓	✓	✓	✓	✓
Score de réputation	✓		✓						
Nom de la règle	✓		✓		✓	✓	✓	✓	✓
Analysé par	✓		✓	✓	✓	✓	✓	✓	✓
Expéditeur	✓		✓	✓	✓	✓	✓	✓	✓
Adresse IP de l'expéditeur	✓	✓	✓						
Serveur	✓		✓	✓	✓	✓	✓	✓	✓
Score de spam	✓		✓						
Objet	✓		✓	✓	✓	✓	✓	✓	✓
Numéro de ticket	✓		✓	✓	✓	✓	✓	✓	✓

Les filtres de recherche **Raison**, **Raisons**, **Etat** et **Tâche** ne sont pas disponibles dans ce tableau de comparaison, car ils sont exclusivement réservés à la catégorie **Eléments détectés** | **Tous les éléments**.

Voir aussi

Types de détection, page 42

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 3-3 Définition des options

Option	Définition
ET	Permet de rechercher des éléments en fonction des conditions définies dans les options de filtrage précédente et suivante, les résultats de la recherche devant remplir les deux conditions.
OU	Permet de rechercher des éléments en fonction des conditions définies dans les options de filtrage précédente et suivante, les résultats de la recherche devant remplir l'une ou l'autre de ces conditions.
Contient	Permet de rechercher un élément contenant le texte spécifié dans le filtre de recherche principal. Par exemple, si vous souhaitez rechercher des éléments mis en quarantaine détectés dans le dossier **Outbox** (Boîte d'envoi), sélectionnez **Dossier** comme filtre de recherche principal, puis **Contient** dans la liste déroulante. Saisissez ensuite `sortant` dans la zone de texte, puis cliquez sur **Rechercher** pour présenter les résultats de la recherche dans la section **Afficher les résultats**.
Ne contient pas	Permet de rechercher un élément qui exclut le texte spécifié des résultats de la recherche. Par exemple, si vous préférez ne pas afficher les éléments consignés dans les résultats de la recherche, sélectionnez **Action entreprise** comme filtre de recherche principal, puis **Ne contient pas** dans la liste déroulante. Saisissez ensuite `journal`, puis cliquez sur **Rechercher** pour présenter les résultats de la recherche dans la section **Afficher les résultats**.
Correspondance exacte	Permet de rechercher un élément qui correspond exactement au texte spécifié. Par exemple, si vous souhaitez rechercher des éléments mis en quarantaine détectés par le numéro de version de **Moteur antivirus** 5400.1158, sélectionnez **Moteur antivirus** comme filtre de recherche principal, puis **Correspondance exacte** dans la liste déroulante. Saisissez ensuite `5400.1158` dans la zone de texte, puis cliquez sur **Rechercher** pour présenter les résultats de la recherche dans la section **Afficher les résultats**.
Correspond à l'expression régulière	Permet de rechercher un élément correspondant à un modèle donné à l'aide d'expressions régulières. Par exemple, si vous souhaitez effectuer une recherche en fonction d'une adresse e-mail valide n'importe où dans la détection, sélectionnez **Nom de la détection** comme filtre de recherche principal, puis **Correspond à l'expression régulière** dans la liste déroulante. Saisissez ensuite `\b[A-Z0-9._%+-]+@(?:[A-Z0-9-]+\.)+[A-Z]{2,4}\b` dans la zone de texte, puis cliquez sur **Rechercher** pour présenter les résultats de la recherche dans la section **Afficher les résultats**.
Egal à	Permet de rechercher un élément contenant une valeur de **Pertinence des spams**, de **Score de réputation** ou de **Score de réputation de l'adresse IP** équivalant à la valeur spécifiée.
Inférieur à	Permet de rechercher un élément contenant une valeur de **Pertinence des spams**, de **Score de réputation** ou de **Score de réputation de l'adresse IP** inférieure à la valeur spécifiée.
Supérieur à	Permet de rechercher un élément contenant une valeur de **Pertinence des spams**, de **Score de réputation** ou de **Score de réputation de l'adresse IP** supérieure à la valeur spécifiée.
Sensible à la casse	Permet de rechercher des éléments en appliquant le critère de sensibilité à la casse.
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 3-3 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.

Voir aussi

Principaux filtres de recherche disponibles, page 44

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.

Vous pouvez utiliser une combinaison de filtres de recherche tels que des opérateurs logiques booléens, des expressions régulières, la sensibilité à la casse ou encore une plage de dates.

Procédure

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 **Spam**, **Hameçonnage** 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 3-4 Options de recherche

Fonctionnalité de recherche	Description
Filtre de recherche principal	Choisissez d'affiner vos critères de recherche en fonction d'un filtre donné tel que **Nom de la stratégie**, **Action entreprise**, **Expéditeur**, etc. Pour plus d'informations sur tous les filtres de recherche principaux, consultez la section *Principaux filtres de recherche disponibles*.
Opérateur logique booléen	Choisissez d'affiner votre recherche en utilisant ces opérateurs logiques : • **ET** • **OU** Pour plus d'informations sur ces options de filtrage, consultez la section *Options de recherche supplémentaires*.
Filtre de recherche secondaire	Choisissez d'affiner votre recherche en utilisant ces filtres secondaires : • **Contient** • **Ne contient pas** • **Correspondance exacte** • **Correspond à l'expression régulière** • **Egal à** • **Inférieur à** • **Supérieur à** Pour plus d'informations sur ces options de filtrage, consultez la section *Options de recherche supplémentaires*.

Tableau 3-4 Options de recherche *(suite)*

Fonctionnalité de recherche	Description
Sensible à la casse	Permet de rechercher des éléments en appliquant le critère de sensibilité à la casse.
Plage de dates	Choisissez d'affiner votre recherche en utilisant toutes les dates ou une période définie. • **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**.

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 diverses actions sur ces éléments mis en quarantaine.

Tableau 3-5 Types d'action

Action	Définition
Libérer	Permet de libérer un élément mis en quarantaine. Sélectionnez un enregistrement applicable dans le volet **Afficher les résultats**, puis cliquez sur **Libérer**. L'e-mail initial est libéré de la base de données et remis au destinataire approprié. • Lorsqu'un élément est téléchargé, libéré ou transféré, il subit une analyse antivirus et figure dans la section **Tableau de bord** | **Eléments récemment analysés**. • Une fois la libération correctement exécutée, l'élément est visible avec le statut **Libéré**, sous la catégorie **Eléments détectés** | **Tous les éléments**.
Télécharger	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**. Vous ne pouvez pas appliquer les options **Télécharger**, **Transférer**, **Afficher** ou **Libérer** à plusieurs enregistrements simultanément à partir de la catégorie **Eléments détectés** | **Tous les éléments**. Cependant, vous pouvez appliquer l'option **Libérer** à plusieurs enregistrements depuis une catégorie donnée.

Tableau 3-5 Types d'action *(suite)*

Action	Définition
Exporter vers un fichier .CSV	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. 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. 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**. • 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.
Transférer	Permet de transférer l'élément mis en quarantaine au destinataire souhaité. Si vous souhaitez le transférer à plusieurs destinataires, séparez les adresses par un point-virgule. Cette action envoie l'élément mis en quarantaine dans un nouvel e-mail, sous forme de pièce jointe (au format `.eml`). Pour transférer l'élément mis en quarantaine à une liste de distribution au sein de votre organisation, spécifiez l'adresse SMTP de la liste de diffusion.
Afficher	Permet d'afficher l'élément mis en quarantaine dans une fenêtre distincte.
Ajouter aux expéditeurs bloqués	Permet d'ajouter l'adresse e-mail d'un expéditeur à la liste des adresses depuis lesquelles l'envoi d'e-mails doit être bloqué (ce que l'on appelle également l'ajout à la liste de blocage).
Ajouter aux expéditeurs autorisés	Permet d'ajouter l'adresse e-mail d'un expéditeur à la liste des adresses depuis lesquelles l'envoi d'e-mails doit être autorisé (ce que l'on appelle également l'ajout à la liste d'autorisation).
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.
Tout sélectionner	Permet de sélectionner tous les éléments mis en quarantaine figurant sur 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 mis en quarantaine figurant dans la section **Afficher les résultats**.
Supprimer	Permet de supprimer les éléments mis en quarantaine que vous avez sélectionnés sur cette page de la section **Afficher les résultats**. Appuyez sur la touche **Ctrl** et maintenez-la enfoncée pour sélectionner plusieurs éléments à la fois.

Tableau 3-5 Types d'action *(suite)*

Action	Définition
Tout supprimer	Permet de supprimer de la base de données tous les éléments mis en quarantaine pour la catégorie sélectionnée.
Eléments affichés **par page**	Permet de spécifier le nombre maximal d'éléments mis en quarantaine à afficher par page. Les options sont les suivantes : • **10** • **20** • **50** • **100**

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

Icône	Description
	Elément mis en quarantaine et pouvant être téléchargé, transféré, libéré ou affiché.
	Elément consigné et impossible à télécharger, à transférer, à libérer ou à afficher.

4 Gestionnaire de stratégies

Permet de configurer ou de gérer différentes stratégies et les actions correspondantes dans le produit. Déterminez la façon dont différents types de menace sont traités une fois détectés.

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 MSME, une stratégie spécifie les paramètres utilisés et les actions entreprises suite au déclenchement d'une détection dans l'environnement Exchange. 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.

Pour simplifier, retenez qu'une stratégie MSME = paramètres de l'analyseur + actions à entreprendre.

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 d'économiser du temps lors de la création et de l'application de stratégies MSME.

Etapes de création d'une stratégie

En tant qu'administrateur, pour créer une stratégie, procédez comme suit :

1. Activez l'analyseur ou le filtre.
2. Modifiez les paramètres de l'analyseur ou du filtre à partir de la stratégie ou de l'option **Ressource partagée**.
3. Spécifiez une action à entreprendre suite au déclenchement d'une détection.
4. Spécifiez les utilisateurs auxquels cette stratégie s'applique.
5. Appliquez les paramètres à la catégorie de stratégies appropriée.

Sommaire

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*) au sein de l'organisation entière.

MSME 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 Exchange.

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

- **A l'accès**
- **A la demande (par défaut)**
- **A la demande (rechercher les virus)**
- **A la demande (supprimer les virus)**
- **A la demande (rechercher le contenu interdit)**
- **A la demande (supprimer le contenu interdit)**
- **A la demande (analyse complète)**
- **Passerelle**

Vous avez la possibilité de personnaliser les stratégies sous chacune de ces catégories afin de gérer avec précision les différentes menaces susceptibles de perturber votre organisation Exchange.

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. MSME entreprend une action concernant un e-mail en fonction des paramètres configurés pour la sous-stratégie dotée de la priorité la plus élevée. Lorsque les règles d'une sous-stratégie ne sont pas satisfaites, MSME passe à la sous-stratégie disposant de la priorité suivante. 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 de sous-stratégies
- Suppression de 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 de sous-stratégies
- Suppression de 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. Dans MSME, 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. Cette stratégie s'applique à tous les utilisateurs au sein d'une organisation.

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

Sous-stratégie

Il s'agit d'une stratégie qui hérite des paramètres et actions d'une autre stratégie. Vous pouvez créer des sous-stratégies supplémentaires, dotées de différents paramètres et actions, en fonction de vos besoins, que vous appliquez à des utilisateurs spécifiques.

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 boîtes aux lettres, de domaines ou de services particuliers de votre organisation. Dans MSME, l'expression générique « groupe de stratégies » est employée pour désigner de telles stratégies.

L'action entreprise concernant un e-mail 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, MSME 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.

Exemple : création d'une sous-stratégie devant être appliquée à tous les e-mails identifiés par MSME comme une menace pour être :

- mis en quarantaine : applicable à tous les utilisateurs ;
- consignés, mis en quarantaine, avec notification de l'administrateur : applicable à tous les administrateurs.

L'exemple simple suivant illustre de manière plus approfondie l'utilité de la mise en place d'une sous-stratégie.

Tableau 4-1 Exemple — Utilité d'une sous-stratégie

Type de stratégie	Analyseur	Niveau de protection	Utilisateurs	Actions à entreprendre
Stratégie principale	Antivirus	Protection moyenne	Tous les utilisateurs	**Quarantaine**
Sous-stratégie	Antivirus	Protection élevée	Administrateurs	**Consigner**, **Quarantaine** et **Notifier l'administrateur**

La restauration du paramètre par défaut de MSME 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 de MSME.

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 utilisateurs ou groupes de votre organisation. Vous pouvez ainsi créer des exceptions et permettre à MSME d'effectuer une analyse particulière.

Exemples de situations où la création d'une sous-stratégie est indiquée :

- Autoriser les e-mails entrants adressés aux utilisateurs de niveau Exécutif de votre organisation après analyse, mais mise en quarantaine des e-mails destinés aux autres utilisateurs.
- Autoriser certains formats de fichier pour des groupes d'utilisateurs précis. Par exemple, vous souhaitez bloquer les fichiers .wav pour tous les utilisateurs, à l'exception d'un service précis de votre organisation.

Procédure

1 Dans le **Gestionnaire de stratégies**, sélectionnez un élément de menu pour lequel vous souhaitez 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** | **Règles**, cliquez sur **Nouvelle règle**.

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 basée sur l'expéditeur ou le destinataire. Vous pouvez créer des règles basées sur les options suivantes :
  - **L'adresse SMTP de l'expéditeur est une adresse e-mail**
  - **L'adresse SMTP de l'expéditeur n'est pas une adresse e-mail**
  - **L'adresse SMTP des destinataires est une adresse e-mail**
  - **L'adresse SMTP des destinataires n'est pas une adresse e-mail**
  - **L'expéditeur est dans le groupe Active Directory**
  - **L'expéditeur n'est pas dans le groupe Active Directory**
  - **Un des destinataires est dans le groupe Active Directory**
  - **Un des destinataires n'est pas dans le groupe Active Directory**

  Assurez-vous de ne pas créer de règles comportant des adresses e-mail ou des noms d'utilisateur incompatibles. Contrairement aux caractères génériques, les expressions régulières ne sont pas prises en charge lors de la spécification des utilisateurs.

- **Copier les règles d'une autre stratégie** : permet de copier les règles à partir d'une autre stratégie.

9 Cliquez sur **Ajouter**.

10 Spécifiez les conditions dans lesquelles la stratégie doit se déclencher pour l'utilisateur. Vous pouvez sélectionner :

- **Au moins une des règles s'applique**
- **Toutes les règles s'appliquent**
- **Aucune règle ne s'applique**

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.

13 Cliquez sur **Terminer**.

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** | **Ressource partagée**.

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, logiciels publicitaires, 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 Exchange, avec l'ajout de 60 nouveaux **Dictionnaires de conformité et DLP**.
Filtrage de fichiers	Permet de créer de nouvelles règles de filtrage de fichiers répondant aux besoins de votre organisation Exchange. Configurez ces paramètres en fonction du nom, de la catégorie ou de la taille des fichiers.
Réputation de l'URL de courrier	Configurez les paramètres pour détecter les URL contenant des liens indésirables, des liens de phishing et des logiciels malveillants.
Antispam	Permet de configurer les paramètres destinés à détecter les e-mails classés comme messages de spam, en fonction du score de spam, de la taille, des règles et des listes de diffusion.
Antiphishing	Permet de configurer les paramètres de rapport concernant les e-mails classés comme messages de phishing.

Les options **Antispam** et **Antiphishing** sont disponibles uniquement si le module complémentaire McAfee Anti-Spam est installé.

Filtres

Activez ou désactivez les filtres suivants et spécifiez les actions à entreprendre en cas de détection, en fonction des besoins de votre organisation Exchange.

Vous pouvez activer ou désactiver certains filtres. En revanche, vous ne pouvez pas configurer les paramètres personnalisés. Ces filtres ne figurent pas dans la liste déroulante disponible sous **Ressource partagée** | **Analyseurs et alertes** | **Analyseurs** | **Catégorie**.

Filtre	Définition
Contenu corrompu	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails au contenu corrompu.
Contenu protégé	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails au contenu protégé.
Contenu chiffré	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails au contenu chiffré.
Contenu signé	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails au contenu signé.
Fichiers protégés par mot de passe	Permet de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails contenant des fichiers protégés par mot de passe. Vous pouvez ignorer la stratégie de filtre de fichier pour autoriser les e-mails contenant des pièces jointes protégées par mot de passe comme requis. Pour plus d'informations, voir *Configuration des paramètres de fichiers protégés par mot de passe*.
Filtrage de taille d'e-mail	Permet de créer ou de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails dont la taille dépasse celle définie dans les options de filtrage de taille d'e-mail. Configurez les paramètres afin de mettre en quarantaine les messages en fonction de la taille globale de l'e-mail, de la taille des pièces jointes et du nombre de pièces jointes.

Filtre	Définition
Contrôle de l'analyseur	Permet de créer ou de configurer les paramètres de l'analyseur de base destinés à définir l'action à entreprendre concernant les e-mails en fonction de leur niveau d'imbrication, de la taille du fichier décompressé et de la durée d'analyse.
Paramètres du courrier MIME	Permet de créer ou de configurer les paramètres destinés à détecter les menaces classées comme messages MIME.
Fichiers HTML	Permet de créer ou de configurer les paramètres destinés à définir l'action à entreprendre concernant les e-mails contenant des éléments HTML tels que des commentaires, des URL, des métadonnées et des scripts.

Divers

Configurez divers paramètres tels que les alertes et les clauses d'exclusion de responsabilité envoyées aux utilisateurs finaux suite à une détection.

Divers	Définition
Paramètres d'alerte	Permet de créer ou de configurer les paramètres applicables à une alerte d'e-mail suite à une détection. Configurez les paramètres tels que le format (HTML ou texte), le codage, le nom de fichier, l'en-tête et le pied de page de l'e-mail d'alerte.
Texte de la clause d'exclusion de responsabilité	Permet de créer ou de configurer le texte de la clause d'exclusion de responsabilité devant figurer dans l'e-mail envoyé à l'utilisateur final suite à une détection.

Tableau de comparaison des analyseurs et des filtres

Cette section présente des informations sur l'analyseur ou le filtre de recherche disponible par défaut pour chaque catégorie de stratégies.

L'analyseur ou le filtre mis à disposition dans MSME varie en fonction de la catégorie de stratégies sélectionnée.

Référez-vous à ce tableau en cas de doute sur l'analyseur ou le filtre disponible pour telle ou telle catégorie de stratégies. En jetant un simple coup d'œil à ce tableau de comparaison, vous prendrez connaissance des analyseurs et des filtres disponibles pour chaque catégorie de stratégies, dont les acronymes utilisés sont les suivants :

- AA — **A l'accès**
- AD (D) — **A la demande (par défaut)**
- AD (RV) — **A la demande (rechercher les virus)**
- AD (SV) — **A la demande (supprimer les virus)**
- AD (RC) — **A la demande (rechercher le contenu non conforme)**
- AD (SC) — **A la demande (supprimer le contenu non conforme)**
- AD (AC) — **A la demande (analyse complète)**
- PS — **Passerelle**

Analyseurs de base

Analyseurs noyaux	AA	AD (D)	AD (RV)	AD (SV)	AD (RC)	AD (SC)	AD (AC)	PS
Analyseur antivirus	✓	✓	✓	✓			✓	
Analyseur de conformité et DLP	✓	✓			✓	✓	✓	
Filtrage de fichiers	✓	✓					✓	
Réputation de l'URL de courrier	✓	✓					✓	
Antispam								✓
Anti-Phishing								✓

Même si l'option **Analyseur de conformité et DLP** est disponible pour les catégories de stratégies **A l'accès** et **A la demande (par défaut)**, elle n'est ni active ni activée par défaut. Vous devez créer les règles requises, puis spécifier une action à entreprendre suite au déclenchement d'une règle et activer l'analyseur.

Filtres

Filtres	AA	AD (D)	AD (RV)	AD (SV)	AD (RC)	AD (SC)	AD (AC)	PS
Contenu corrompu	✓	✓					✓	
Contenu protégé	✓	✓			✓	✓	✓	
Contenu chiffré	✓	✓			✓	✓	✓	
Contenu signé	✓	✓			✓	✓	✓	
Fichiers protégés par mot de passe	✓	✓			✓	✓	✓	
Filtrage de taille d'e-mail	✓							✓
Contrôle de l'analyseur	✓	✓	✓	✓	✓	✓	✓	✓

Filtres	AA	AD (D)	AD (RV)	AD (SV)	AD (RC)	AD (SC)	AD (AC)	PS
Paramètres du courrier MIME	✓	✓			✓		✓	✓
Fichiers HTML	✓	✓			✓		✓	✓

Paramètres d'alerte et de clause d'exclusion de responsabilité

Paramètres divers	AA	AD (D)	AD (RV)	AD (SV)	AD (RC)	AD (SC)	AD (AC)	PS
Paramètres d'alerte	✓	✓		✓	✓	✓	✓	✓
Texte de la clause d'exclusion de responsabilité	✓							

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.
Le type de paramètres disponibles dépend de la stratégie sélectionnée.

Procédure

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 de votre choix.

La page des stratégies correspondante s'affiche. Les filtres applicables sont disponibles dans les pages de stratégie respectives.

3 La page de stratégies inclut 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 utilisateurs** : permet de spécifier les règles de stratégie qui s'appliquent à des utilisateurs précis.

Vous pouvez spécifier des utilisateurs pour les sous-stratégies uniquement.

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

Tableau 4-2 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 4-2 Configuration de la stratégie *(suite)*

Option	Définition
Analyseurs noyaux	Permet de configurer la stratégie de chacun des analyseurs suivants : • **Analyseur antivirus** • **Analyseur de conformité et DLP** • **Filtrage de fichiers** • **Réputation de l'URL de courrier** • **Antispam** • **Anti-Phishing**
Filtres	Permet de configurer la stratégie de chacun des filtres suivants : • **Contenu corrompu** • **Contenu protégé** • **Contenu chiffré** • **Contenu signé** • **Fichiers protégés par mot de passe** • **Filtrage selon la taille du courrier** • **Contrôle de l'analyseur** • **Paramètres du courrier MIME** • **Fichiers HTML**
Paramètres divers	Permet de configurer les paramètres d'alerte et les messages de clause d'exclusion de responsabilité pour les stratégies. Les options **diverses** incluent : • **Paramètres d'alerte** • **Texte d'avis de non-responsabilité**

Ajout d'un analyseur ou d'un filtre

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

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 ;
- uniquement activé pendant une plage horaire précise.

Procédure

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**.

L'option **Ajouter un analyseur/filtre** est uniquement disponible pour les catégories de stratégies **A l'accès** et **Passerelle**.

4 Dans la liste déroulante **Spécifier la catégorie**, sélectionnez l'analyseur ou le filtre requis.

5 Dans la section **Quand utiliser cette instance**, sélectionnez une plage horaire existante ou créez-en un nouvelle.

6 Cliquez sur **Enregistrer**.

7 Cliquez sur **Appliquer**.

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

Création d'une règle pour un utilisateur spécifique

Elaborez de nouvelles règles et spécifiez les conditions à appliquer à un utilisateur donné.

Vous avez la possibilité de créer des règles pour des utilisateurs ou des groupes spécifiques afin de définir une exception à la stratégie.

Procédure

1 Dans le **Gestionnaire de stratégies**, sélectionnez une catégorie de stratégies.

2 Cliquez sur la sous-stratégie que vous souhaitez configurer pour des utilisateurs spécifiques.

3 Cliquez sur l'onglet **Spécifier des utilisateurs**.

4 Cliquez sur **Nouvelle règle**.

5 Dans la section **Spécifier une règle de stratégie**, vous pouvez choisir ce qui suit :

- **<sélectionnez un modèle de règle>** : permet de spécifier une règle de stratégie basée sur l'expéditeur ou le destinataire. Vous pouvez créer des règles basées sur les options suivantes :
  - **L'adresse SMTP de l'expéditeur est une adresse e-mail**
  - **L'adresse SMTP de l'expéditeur n'est pas une adresse e-mail**
  - **L'adresse SMTP des destinataires est une adresse e-mail**
  - **L'adresse SMTP des destinataires n'est pas une adresse e-mail**
  - **L'expéditeur est dans le groupe Active Directory**
  - **L'expéditeur n'est pas dans le groupe Active Directory**
  - **Un des destinataires est dans le groupe Active Directory**
  - **Un des destinataires n'est pas dans le groupe Active Directory**

  Assurez-vous de ne pas créer de règles comportant des adresses e-mail ou des noms d'utilisateur incompatibles. Contrairement aux caractères génériques, les expressions régulières ne sont pas prises en charge lors de la spécification des utilisateurs.

- **Copier les règles d'une autre stratégie** : permet de copier les règles à partir d'une autre stratégie.

6 Cliquez sur **Ajouter**.

7 Spécifiez les conditions de déclenchement de la stratégie pour l'utilisateur. Vous pouvez sélectionner :

- **Au moins une des règles s'applique**
- **Toutes les règles s'appliquent**
- **Aucune règle ne s'applique**

8 Cliquez sur **Appliquer** pour enregistrer la règle pour l'utilisateur spécifique.

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 le comportement à adopter lorsqu'un e-mail ou sa pièce jointe déclenche une détection.

Lorsqu'une règle de stratégie est déclenchée d'après les paramètres d'analyseur ou de filtre, MSME 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 consiste à supprimer l'e-mail ayant déclenché une détection, l'action secondaire peut consister à consigner la détection dans un journal et à notifier l'administrateur.

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 4-3 Actions principales

Action	Définition
Tenter de nettoyer tout virus ou cheval de Troie détecté	Permet de nettoyer l'e-mail contenant un virus ou un cheval de Troie détecté par l'**Analyseur antivirus**.
Remplacer l'élément par une alerte	Remplace par une alerte l'e-mail ayant déclenché la détection.
Supprimer l'élément incorporé	Supprime la pièce jointe ayant déclenché la détection dans un e-mail.
Supprimer le message	Supprime l'e-mail ayant déclenché la détection.
Autoriser	Autorise l'e-mail à passer à la phase d'analyse suivante ou à atteindre l'utilisateur final.
Action basée sur le score	Permet d'entreprendre une action basée sur le score de spam. Cette action est uniquement disponible pour l'analyseur antispam ; vous devez alors sélectionner la valeur à attribuer à l'option **Si le score de spam est** (Elevé, Moyen ou Faible).
Router vers le dossier Courrier indésirable du système	Permet d'acheminer l'e-mail détecté par l'analyseur **Antispam** jusqu'à l'adresse e-mail spécifiée sous **Paramètres et diagnostics** | **Antispam** | **Filtrage du spam au niveau de la passerelle** | **Adresse du dossier Courrier indésirable du système**.
Router vers le dossier Courrier indésirable de l'utilisateur	Permet d'acheminer l'e-mail détecté par l'analyseur **Antispam** jusqu'au dossier **Courrier indésirable** du destinataire.
Rejeter le message	Permet de rejeter l'e-mail et d'envoyer une notification à l'utilisateur.
Remplacer la pièce jointe par une alerte	Permet de remplacer la pièce jointe à un e-mail par une alerte lorsque l'analyseur **Filtrage selon la taille du courrier** est déclenché suite au dépassement de la taille maximale de la pièce jointe.
Remplacer toutes les pièces jointes par une seule alerte	Permet de remplacer l'e-mail contenant plusieurs pièces jointes par une alerte unique lorsque l'analyseur **Filtrage selon la taille du courrier** est déclenché suite au dépassement du nombre maximal de pièces jointes.
Ne pas permettre que des modifications cassent la signature	Permet d'empêcher MSME de casser la signature lorsqu'un e-mail au **contenu signé** est détecté.
Autoriser les modifications pour casser la signature	Permet d'autoriser MSME à casser la signature lorsqu'un e-mail au **contenu signé** est détecté.

Tableau 4-4 Actions secondaires

Action	Définition
Consigner	Permet d'enregistrer la détection dans un journal.
Quarantaine	Permet de conserver dans la base de données de quarantaine une copie de l'e-mail 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. Sélectionnez **Transférer l'e-mail mis en quarantaine** afin d'envoyer l'e-mail à un réviseur ou à une liste de distribution spécifique en fonction de la catégorie de détections. Pour configurer les notifications d'après la catégorie de détections, accédez à **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Avancé**. L'option **Transférer l'e-mail mis en quarantaine** ne s'applique pas aux stratégies **Analyseur antivirus** ou **Passerelle**.
Notifier l'administrateur	Permet d'envoyer une copie de l'e-mail à l'administrateur spécifié sous **E-mail de l'administrateur** via **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **Général**.
Notifier l'expéditeur interne	Permet d'envoyer un message d'alerte à l'expéditeur interne lorsque l'e-mail d'origine provient du domaine faisant autorité de votre serveur Exchange.
Avertir l'expéditeur externe	Permet d'envoyer un message d'alerte à l'expéditeur lorsque l'e-mail d'origine ne provient pas du domaine faisant autorité de votre serveur Exchange.
Notifier le destinataire interne	Permet d'envoyer un message d'alerte au destinataire lorsque ce dernier fait partie du domaine faisant autorité de votre serveur Exchange.
Avertir le destinataire externe	Permet d'envoyer un message d'alerte au destinataire lorsque ce dernier ne fait pas partie du domaine faisant autorité de votre serveur Exchange.

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**.

Par exemple, si vous souhaitez employer une clause d'exclusion de responsabilité différente pour les destinataires internes et externes, créez des clauses distinctes et appliquez-les dans la sous-stratégie appropriée.

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 Exchange.

Procédure

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 4-5 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.
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 dans les cas suivants : • Il s'agit d'un analyseur par défaut. • 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**.

Vous avez à présent terminé la configuration des paramètres d'un analyseur en fonction des exigences de votre organisation Exchange.

Configuration des paramètres d'alerte

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

Procédure

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 4-6 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. Pour plus d'informations sur les variables que vous pouvez utiliser dans les alertes, consultez la section *Champs de notification disponibles*.
Supprimer	Permet de supprimer les paramètres de l'analyseur. Vous ne pouvez pas supprimer une alerte dans les cas suivants : • Il s'agit d'une alerte d'analyseur par défaut. • 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 Exchange.

Créer une alerte

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

Procédure

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 Renseignez le champ **Nom de l'alerte** en utilisant un nom explicite.

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

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

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

Tableau 4-7 Options de la barre d'outils

Options	Description
Gras	Permet d'afficher le texte sélectionné en gras.
Italique	Permet d'afficher le texte sélectionné en italique.
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 tout en étant alignées à droite et à gauche.
Liste classée	Permet de transformer le texte sélectionné en liste numérotée.
Liste non classée	Permet de transformer le texte sélectionné en 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	Permet d'insérer une ligne horizontale.
Insérer un lien	Permet d'insérer un lien hypertexte à l'endroit où se trouve 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 se trouve 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	Pour insérer un tableau à la position actuelle du 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**.

8 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 —** Pour afficher le contenu sous la forme de texte brut.

  Vous pouvez utiliser les champs de notification suivants pour les inclure dans votre message d'alerte. Par exemple, si vous voulez afficher dans le message d'alerte le nom de l'élément détecté et l'action entreprise lors de sa détection, utilisez **%vrs%** et **%act%** sur la page **Editeur d'alerte**. Pour plus d'informations sur les options des champs de notification, consultez la section *Champs de notification disponibles*.

McAfee recommande d'enregistrer les fichiers journaux au format texte simple afin de permettre à chaque client de messagerie d'afficher le contenu.

9 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 Exchange.

Procédure

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 **Sélectionner une langue**, sous la section **Règles de conformité et DLP**, sélectionnez la langue.

Vous pouvez également afficher et modifier tous les dictionnaires des langues prises en charge. (Les langues prises en charge sont le chinois simplifié, le français, l'allemand, le japonais et l'espagnol.)

4 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 4-8 Définition des options

Option	Définition
Catégorie	Permet de sélectionner l'analyseur requis à configurer. Cette distribution comprend 60 dictionnaires de conformité et DLP supplémentaires, garantissant que le contenu de l'e-mail est conforme aux stratégies de confidentialité et de conformité de votre organisation. Caractéristiques des 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, code source (Java, C++, etc.) Ces dictionnaires sont classés par catégories : • Dictionnaires basés sur le score : une règle est déclenchée lorsqu'un e-mail 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 l'e-mail.
Nouvelle catégorie	Permet de créer un nouveau dictionnaire de **Règles de conformité et DLP**. Toute nouvelle catégorie ou condition créée ne dépend pas du score.
Créer une nouvelle catégorie	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.
Modifier	Permet de modifier les paramètres de la règle **Conformité et DLP** sélectionnée.
Supprimer	Permet de supprimer la règle **Conformité et DLP**. Vous ne pouvez pas supprimer une règle **Conformité et DLP** dans les cas suivants • Elle est activée. Désélectionnez la règle, cliquez sur **Appliquer** pour appliquer les paramètres, puis choisissez **Supprimer**. • Elle est utilisée 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.

5 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.

6 Tapez le **Nom de la règle** et sa **Description**.

7 Sélectionnez **Ajouter cette règle au groupe de règles de cette catégorie** pour ajouter la nouvelle règle au groupe de règles pour la catégorie sélectionnée.

8 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 est désactivée pour certaines expressions.
- Pour plus d'informations, reportez-vous à http://www.regular-expressions.info/reference.html ou à http://www.zytrax.com/tech/web/regex.htm.

- **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.)
- **Débute 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**.

9 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.

10 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.

11 Sélectionnez **Au sein d'un bloc** pour indiquer le nombre de **Caractères** d'un bloc à analyser.

12 Cliquez sur **Ajouter un mot contextuel** pour taper des mots ou des expressions supplémentaires.

13 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**.

14 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.

15 Si vous n'avez pas sélectionné **Tout**, cliquez sur **Effacer les sélections** pour désélectionner l'une des options de type de fichier sélectionnées.

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

17 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 Exchange.

Configuration des règles de filtrage de fichiers

Créez de nouvelles règles destinées à détecter les fichiers en fonction de leur nom, de leur type ou de leur taille.

Avant de commencer

La règle de filtrage de fichiers se déclenche uniquement lorsque vous sélectionnez une condition. Assurez-vous de créer une règle propre à chacune des catégories suivantes :

- Nom du fichier
- Catégorie de fichier
- Taille du fichier

La procédure suivante fournit des informations sur la configuration des trois catégories. Selon les exigences de votre organisation Exchange, sélectionnez une seule catégorie par règle de filtrage de fichiers et créez des règles distinctes pour les différentes catégories. Si une règle contient plusieurs critères comme **Filtrage par nom de fichier**, **Filtrage par catégorie de fichier**, et **Filtrage de tailles de fichier**, tous les critères doivent être satisfaits pour déclencher la règle.

Procédure

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

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

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

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 Activez l'option **Evaluation des éléments dans les fichiers d'archive**.

Sélectionnez cette option si la règle Filtre de fichiers est applicable pour l'analyse des fichiers d'archive. Lorsque vous activez cette règle, les règles Filtre de fichiers suivantes sont appliquées aux fichiers d'archive.

6 La page **Règle de filtrage des fichiers** inclut les options suivantes :

Tableau 4-9 Définition des options — Filtrage par nom de fichier

Option	Définition
Activer le filtrage des 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 4-10 Définition des options — Filtrage des catégories de fichiers

Option	Définition
Activer le filtrage des 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.
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.

Pour autoriser les fichiers .zip protégés par mot de passe et qui contiennent des fichiers restreints, assurez-vous que la **Règle de contournement protégée par mot de passe** apparaît tout en haut de la liste.

Tableau 4-11 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 : • **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.

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

8 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 en fonction des exigences de votre organisation Exchange.

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 Exchange.

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, MSME comprend les plages horaires suivantes :

- **En permanence**
- **En semaine**
- **Les week-ends**

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

Procédure

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 **Créneaux horaires**.

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 Exchange.

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**
- **Antispam**
- **Antihameçonnage**

Procédures

- *Configuration des paramètres de l'analyseur antivirus*, page 77
  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 d'analyseur de conformité et DLP*, page 80
  Configurez les paramètres de l'**Analyseur de conformité et DLP** dans une stratégie afin d'identifier les données textuelles non conformes dans un e-mail ou une pièce jointe et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de filtrage de fichiers*, page 82
  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.
- *Configurer les paramètres de réputation de l'URL de courrier*, page 83
  Configurez les paramètres de **Réputation de l'URL de courrier** pour détecter les URL malveillantes dans le corps de l'e-mail.
- *Vérification de la réputation TIE des pièces jointes aux e-mails*, page 86
  MSME fournit désormais une fonctionnalité supplémentaire de détection des menaces qui exploite la fonction de vérification de la réputation TIE pour les pièces jointes à des e-mails au niveau de la passerelle, du concentrateur et de la boîte aux lettres.
- *Configuration des paramètres TIE pour l'analyse des pièces jointes aux e-mails*, page 88
  Activez la vérification de la réputation TIE pour les pièces jointes aux e-mails en fonction de la catégorie de réputation des fichiers.
- *Configuration des paramètres antispam*, page 89
  Configurez les paramètres dans une stratégie afin de détecter les e-mails de spam et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres antiphishing*, page 93
  Configurez les paramètres dans une stratégie afin de bloquer les messages de phishing (hameçonnage) à l'aide du moteur et des règles antispam et d'entreprendre les actions nécessaires.

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

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

La page de stratégie de 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.
- Si vous ajoutez un nouvel analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Les options suivantes sont disponibles dans la section **Options** :

Option	Définition
Protection élevée	Permet d'analyser tous les fichiers, fichiers d'archive, virus inconnus, virus de macro inconnus, virus de mass-mailing 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, virus de mass-mailing et programmes potentiellement indésirables.
Protection faible	Permet d'analyser uniquement les types de fichier par défaut, les fichiers d'archive, les virus de mass-mailing et les programmes potentiellement indésirables.
<create new set of 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 Dans l'onglet **Options de base**, sous **Spécifier les fichiers à analyser**, sélectionnez l'une des options suivantes :

- **Analyser tous les fichiers** — Permet de spécifier que tous les fichiers doivent être analysés, quel que soit leur type.
- **Types de fichiers par défaut** — Permet de spécifier que seuls les types de fichier par défaut doivent être analysés.
- **Types de fichiers définis** — Permet de spécifier les types de fichier à analyser.

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

- **Analyser des fichiers d'archives (ZIP, ARJ, RAR…)**
- **Détecter les virus de fichiers inconnus**
- **Détecter les virus de macros inconnus**
- **Activez le service de réputation des fichiers McAfee Global Threat Intelligence** — Cette option active les renseignements sur les menaces recueillis par McAfee Labs pour empêcher les dommages et le vol de données avant même qu'une mise à jour de signature soit disponible. Sélectionnez le niveau de sensibilité dans les options disponibles.
- **Rechercher les macros dans tous les fichiers**
- **Rechercher toutes les macros et les considérer comme infectées**
- **Supprimer toutes les macros des fichiers de documents**

Les options **Rechercher toutes les macros et les considérer comme infectées** et **Supprimer toutes les macros des fichiers de documents** offrent une fonctionnalité combinée. Lorsque vous sélectionnez **Rechercher toutes les macros et les considérer comme infectées**, l'option **Supprimer toutes les macros des fichiers de documents** est automatiquement sélectionnée. Lorsque vous activez cette option, toutes les macros présentes dans les pièces jointes sont traitées comme infectées.

9 Dans l'onglet **Avancé**, sous **Catégories personnalisées de programmes malveillants**, spécifiez les éléments à traiter comme des logiciels malveillants. Deux modes de sélection des types de logiciels malveillants sont disponibles :

- 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 Dans 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 Dans l'onglet **Programmes potentiellement indésirables**, 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**. Dans les onglets suivants, spécifiez les actions d'analyseur antivirus à exécuter en cas de détection d'un virus (ou un comportement de type viral) :

- **Nettoyage** : sélectionnez **Tenter de nettoyer tout virus ou cheval de Troie détecté** pour activer diverses actions. Sélectionnez les actions à entreprendre à partir des options suivantes :
  - **Consigner**
  - **Quarantaine**
  - **Notifier l'administrateur**
  - **Notifier l'expéditeur interne**
  - **Avertir l'expéditeur externe**
  - **Notifier le destinataire interne**
  - **Avertir le destinataire externe**
- **Actions par défaut** : dans la liste déroulante **Entreprendre l'action suivante**, sélectionnez une action.
  - **Remplacer l'élément par une alerte**
  - **Supprimer l'élément incorporé**
  - **Supprimer le message**
  - **Autoriser**

Pour plus d'informations sur les actions principales et secondaires, consultez la section *Actions pouvant être entreprises concernant les détections*.

16 Sélectionnez le document d'alerte correspondant ou cliquez sur **Créer** pour créer un nouveau document d'alerte. Dans la section **Et aussi**, sélectionnez les autres actions à exécuter pour les onglets suivants :

- **Programme malveillant personnalisé**
- **Packers**
- **Programme potentiellement indésirable**

17 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

18 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 textuelles non conformes dans un e-mail ou une pièce jointe et d'entreprendre les actions nécessaires correspondantes.

Procédure

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**.
- 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.
- Si vous ajoutez un nouvel analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

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 message d'alerte lorsque le contenu d'un e-mail est remplacé suite au déclenchement d'une règle. Voir *Créer une alerte* pour plus d'instructions.
- **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 Dans **Spécifier les actions à associer à la règle**, sélectionnez la langue à partir du menu déroulant **Sélectionner une langue**.

Vous pouvez également afficher et modifier tous les dictionnaires des langues prises en charge. (Les langues prises en charge sont le chinois simplifié, le français, l'allemand, le japonais et l'espagnol.)

Par exemple, lorsque MSME est installé en allemand, vous pouvez toujours afficher et modifier les dictionnaires des langues prises en charge. Toute nouvelle catégorie que vous créez est disponible pour toutes les langues prises en charge.

8 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. La valeur est supérieure au score de seuil défini. De ce fait, la règle est déclenchée.

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 e-mail.

9 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 e-mail.

10 Sous **Mais également**, sélectionnez une ou plusieurs actions.

11 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

12 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

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.
- Si vous ajoutez un analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Sélectionnez **Rechercher les fichiers incorporés** pour analyser les e-mails incorporés.

6 Dans la section **Sélection d'alerte**, cliquez sur :

- **Créer** : permet de créer un nouveau message d'alerte lorsque la pièce jointe d'un e-mail est remplacée suite au déclenchement d'une règle. Voir *Créer une alerte* pour plus d'instructions.
- **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.

7 Dans la section **Règles de filtrage des fichiers et actions associées**, dans le menu déroulant **Règles disponibles**, sélectionnez une règle disponible. Pour 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*.

Les paramètres de filtrage de fichiers peuvent bloquer les fichiers restreints comme les fichiers .exe présentés sous la forme de pièce jointe d'e-mail. Si le fichier .exe est envoyé sous la forme d'un fichier .zip protégé par mot de passe, et bien que le paramètre **Fichiers protégés par mot de passe** soit configuré pour autoriser le fichier, la règle de filtrage de fichiers peut bloquer ce fichier.

Parfois, vous devrez peut-être autoriser les fichiers restreints légitimes présentés sous la forme de fichiers .zip protégés par mot de passe. Pour autoriser le fichier .zip protégé par mot de passe qui contient des fichiers restreints comme des fichiers .exe, vous devez ajouter la **Règle de contournement de protection par mot de passe** à partir de la liste déroulante **Règles disponibles**.

Assurez-vous que cette règle est la première règle de la liste. Si la règle est répertoriée à un autre niveau, supprimez-la, puis sélectionnez-la dans la liste déroulante **Règles disponibles**.

Assurez-vous de créer des règles de filtrage de fichiers distinctes pour chaque catégorie (nom de fichier, type et taille, etc.).

8 Cliquez sur **Modifier** pour indiquer les actions à entreprendre suite au déclenchement de l'analyseur par un fichier ou une pièce jointe dans un e-mail.

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

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

Configurer les paramètres de réputation de l'URL de courrier

Configurez les paramètres de **Réputation de l'URL de courrier** pour détecter les URL malveillantes dans le corps de l'e-mail.

Une fois activé, MSME analyse chaque URL dans le corps de l'e-mail, obtient le score de réputation, compare le score au seuil défini, et effectue l'action adéquate.

Le logiciel traite le message avant qu'il ne pénètre dans l'organisation en retirant les URL du corps de l'e-mail. Si un e-mail contient plusieurs URL, et qu'une de ces URL dépasse le seuil défini, l'action est effectuée sur l'e-mail conformément à la configuration.

L'activation de cette fonctionnalité protège votre système des menaces comme les attaques de déni de service (DoS), les liens de phishing, les URL contenant des logiciels malveillants ou les URL indésirables.

La fonctionnalité Réputation de l'URL de courrier est disponible pour ces stratégies :

- **A l'accès**
- **A la demande (par défaut)**, et
- **A la demande (analyse complète)**

Selon l'option de configuration que vous avez sélectionnée pendant l'installation du logiciel, la réputation de l'URL de courrier est activée ou désactivée par défaut pour les stratégies :

- Pour la **Configuration par défaut** — Désactivée pour toutes les stratégies.
- Pour la **Configuration améliorée** — Activée uniquement pour les stratégies d'analyse à l'accès.

Lorsque vous activez l'option **Réputation de l'URL de courrier** pour la première fois, le logiciel télécharge le cache local des URL à partir du serveur McAfee GTI.

Pour chaque URL, le logiciel vérifie le score de réputation auprès de la base de données locale et effectue l'action adéquate selon la configuration. Si le score de réputation n'est pas disponible au sein de la base de données locale, le logiciel obtient le score auprès du serveur McAfee GTI. Le logiciel vérifie auprès du serveur McAfee GTI et met à jour la base de données locale à intervalles réguliers. Si la base de données locale n'est pas mise à jour pendant 30 jours, le logiciel télécharge l'ensemble de la base de données lors de la mise à jour suivante. Dans le cas contraire, la mise à jour est incrémentielle. Par défaut, la base de données locale est mise à jour une fois par jour, tous les jours. Vous ne pouvez pas modifier l'emplacement du stockage de la base de données.

Vous ne pouvez pas mettre à jour la base de données locale à l'aide de ePolicy Orchestrator, car le serveur a besoin de connexions Internet directes. Toutefois, si vous utilisez le serveur proxy pour télécharger les règles antispam, la même configuration peut être utilisée pour télécharger la base de données d'URL.

Procédure

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

La protection **Réputation de l'URL de courrier** est disponible uniquement pour les stratégies **A l'accès**, **A la demande (par défaut)**, et **A la demande (analyse complète)**.

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

3 A partir d'**Activation**, sélectionnez **Activer**.

- 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.
- Si vous ajoutez un nouvel analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

4 Dans la liste déroulante **Options**, vous pouvez sélectionner :

- **Paramètres d'URL de courrier par défaut** — Pour appliquer les valeurs de seuil par défaut.
- **Créer un nouveau jeu d'options** — Pour définir les valeurs de seuil comme requis.

> Si vous modifiez les paramètres existants, assurez-vous de fournir un **Nom de l'instance** unique pour les paramètres de l'analyseur.

5 Pour définir les paramètres de l'analyseur, sélectionnez **Créer un nouveau jeu d'options**.

6 Sur la page **Réputation de l'URL de courrier**, définissez ces valeurs, puis cliquez sur **Enregistrer**.

- **Nom de l'instance**
- **Seuil supérieur de réputation d'URL**
- **Seuil inférieur de réputation d'URL**
- **Nombre maximum d'URL par e-mail**

> La valeur **Seuil supérieur de réputation d'URL** doit être supérieure à la valeur **Seuil inférieur de réputation d'URL**.

> Si une URL apparaît plusieurs fois, l'URL comptée est 1, et non le nombre d'occurrences. Par exemple, si l'e-mail contient 50 URL et qu'une URL apparaît 20 fois, la somme des URL est 31 et non 50.

7 Pour la section **Actions à entreprendre**, cliquez sur **Modifier** pour définir les actions.

> Vous pouvez également appliquer les paramètres par défaut.

8 Sur la page **Actions de réputation de l'URL de courrier**, définissez ces paramètres pour **Si le score de réputation de l'URL de courrier dépasse le seuil supérieur**, **Si le score de réputation de l'URL de courrier est inférieur au seuil supérieur**, et **Lorsque le nombre d'URL de courrier dépasse la limite**.

a A partir de la liste déroulante **Entreprendre l'action suivante**, sélectionnez :

- **Remplacer l'élément par une alerte**.
- **Supprimer le message**.
- **Autoriser**.

Lorsque vous sélectionnez **Remplacer l'élément par une alerte**, sélectionnez le format d'alerte :

- **Alerte de réputation de l'URL de courrier par défaut** — Pour utiliser le message d'alerte par défaut.
- **Créer** — Pour définir le message d'alerte comme vous le souhaitez. Saisissez un nom unique pour le **Nom de l'alerte**, définissez le message d'alerte, définissez le format de texte à partir de la liste déroulante **Afficher**, puis cliquez sur **Enregistrer**.

> McAfee recommande d'enregistrer les alertes au format texte simple afin de permettre à tous les clients de messagerie d'afficher le contenu texte.

b A partir de la section **Et aussi**, définissez ces options :

- **Consigner**
- **Quarantaine**
- **Notifier l'expéditeur interne**
- **Avertir l'expéditeur externe**

- **Transférer l'e-mail mis en quarantaine**
- **Notifier l'administrateur**
- **Notifier le destinataire interne**
- **Avertir le destinataire externe**

Pour la définition de chacune de ces options, voir *Actions pouvant être entreprises concernant les détections*.

9 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

10 Cliquez sur **Appliquer** pour implémenter ces paramètres dans une stratégie.

Vous pouvez afficher les URL détectées à partir de la page **Eléments détectés** | **Réputation de l'URL de courrier**. Dans la section **Afficher les résultats**, vous pouvez afficher la liste des URL détectées. Cliquez sur **URL bloquées** dans la colonne **Phrases interdites** pour un affichage détaillé.

Exemples de seuils supérieur et inférieur de réputation d'URL

Définissez la valeur **Seuil supérieur de réputation d'URL** sur `80` et la valeur **Seuil inférieur de réputation d'URL** sur `50`. Si le score de réputation de l'URL est :

Score de réputation GTI de	Action
Supérieur à 80	Une action est effectuée conformément aux paramètres de réputation de l'URL de courrier.
Inférieur à 50	MSME autorise l'e-mail avec l'URL.
Entre 50 et 80	MSME suspecte que l'URL peut être malveillante et agit selon les paramètres.

La valeur du seuil **Fortement suspect** détecte les URL malveillantes les plus dangereuses. Lorsque vous réduisez la valeur du seuil, les chances d'obtenir un faux positif augmentent. Faux positif – Une URL peut être légitime, mais la base de données la considère comme une URL malveillante potentielle.

Vérification de la réputation TIE des pièces jointes aux e-mails

MSME fournit désormais une fonctionnalité supplémentaire de détection des menaces qui exploite la fonction de vérification de la réputation TIE pour les pièces jointes à des e-mails au niveau de la passerelle, du concentrateur et de la boîte aux lettres.

Qu'est-ce que TIE ?

Threat Intelligence Exchange améliore les fonctionnalités de protection et de détection en temps réel, en réalisant une vérification complète et avancée de la réputation des fichiers tout en empêchant la propagation des menaces. Le serveur TIE analyse rapidement les pièces jointes au niveau de la passerelle, du concentrateur et de la boîte aux lettres. Pour plus d'informations sur Threat Intelligence Exchange, reportez-vous au *Guide Produit de Threat Intelligence Exchange 2.0*.

La réputation TIE repose sur deux variantes :

- Réputation des certificats
- Réputation des fichiers

TIE commence par valider le score de réputation des fichiers ou des certificats. Si seule la réputation des certificats est Malveillant connu, le score de réputation des fichiers est pris en compte.

Fonctionnement de MSME avec TIE

Lorsque TIE est activé dans les paramètres de stratégie, après l'application de règles de filtrage de fichiers, MSME vérifie la réputation des pièces jointes aux e-mails auprès du serveur TIE. D'après la réputation TIE du fichier, les scores sont mappés vers l'une de ces catégories, et MSME exécute l'action spécifiée dans la configuration de cette catégorie :

- Approuvé connu - 99
- Très probablement approuvé - 85
- Peut-être approuvé - 70
- Inconnu - 50
- Peut-être malveillant - 30
- Très probablement malveillant - 15
- Malveillant connu - 1

Lorsque vous configurez une action pour une catégorie spécifique, la même action est appliquée à toutes les catégories dont le score de réputation TIE est inférieur à la catégorie spécifiée. Par défaut, la valeur **Exécuter des actions si la réputation est égale ou inférieure à** est définie sur **Peut-être malveillant**.

Par exemple, lorsque vous définissez **Exécuter des actions si la réputation est égale ou inférieure à** sur **Inconnu** et l'action sur **Remplacer l'élément par une alerte** pour les fichiers dont le score est de 50, toutes les pièces jointes avec un score de réputation TIE de 50 ou moins sont remplacées par un message d'alerte. Vous pouvez également sélectionner des actions secondaires pour l'alerte.

Les scores de réputation sont mis en cache en local et MSME peut utiliser le cache local mis à jour pour les vérifications de la réputation.

Lorsque TIE est désactivé, l'action d'analyse est exécutée conformément aux paramètres de stratégie. Lorsque TIE est activé, mais que le serveur TIE est injoignable et que le cache local ne contient aucune entrée pour le fichier, la vérification de la réputation à partir de TIE est ignorée et l'e-mail est analysé conformément aux paramètres de stratégie.

Pour plus d'informations sur le mappage du score de réputation, consultez le *Guide Produit de TIE*.

MSME envoie uniquement les fichiers des types ci-dessous pour vérification de la réputation TIE :

- EXE
- PDF
- Documents Microsoft Office

Pour consulter la liste des types de fichiers pris en charge, reportez-vous à l'article KB89578.

Lorsque l'e-mail contient une pièce jointe compressée, le fichier compressé est extrait et seuls les fichiers présents dans la pièce jointe et correspondant aux types pris en charge sont envoyés pour vérification de la réputation TIE. Pour obtenir la liste des types de fichiers compressés pris en charge, reportez-vous à l'article KB89577.

Dans le cadre de la vérification des autres types de fichiers et de la post-vérification de la réputation TIE, MSME analyse les pièces jointes conformément aux paramètres de stratégie. Lorsque vous libérez l'élément mis en quarantaine suite à une détection TIE, le fichier est analysé à la recherche d'éventuels virus uniquement avant d'être autorisé. Vous pouvez consulter le nombre de fichiers détectés par TIE et le nombre de fichiers envoyés à ATD dans la page Tableau de bord.

Utilisation de la réputation Advanced Threat Defense

Vous pouvez également activer la détection Advanced Threat Defense pour les catégories de réputation sélectionnées pour les fichiers et en fonction de la taille de la pièce jointe.

Lorsque la réputation TIE d'un fichier est vérifiée, TIE renvoie le score de réputation et recommande parfois d'analyser le fichier. MSME envoie le fichier à Advanced Threat Defense en fonction de la catégorie et de la taille de fichier configurées. Si un score de réputation révisé est disponible pour le fichier, le cache local est mis à jour avec ce score. Le score révisé sera utilisé à partir de la recherche suivante. Le valeur par défaut du paramètre **Exécuter des actions si la réputation est égale ou inférieure à** est **Peut-être malveillant** et celle de **Taille du fichier** est 8 Mo.

Paramètres recommandés pour le déploiement d'un serveur TIE pour MSME

McAfee recommande de :

- Déployer un serveur TIE dans une configuration secondaire afin de traiter toutes les demandes de réputation TIE provenant de MSME dans le même centre de données que le serveur Exchange. Le serveur TIE peut ainsi traiter un maximum de pièces jointes par seconde dans une infrastructure dédiée.

  Chaque pièce jointe envoyée pour vérification de la réputation TIE invoque un maximum de 2 demandes TIE.

- Le trafic de réputation est moindre lorsque le serveur MSME met en cache local les réputations. Toutefois, des pics peuvent avoir lieu étant donné que MSME efface le cache local après le redémarrage du service.
- Utilise les compteurs inclus dans le tableau de bord MSME pour estimer les demandes provenant de MSME. Pour plus d'informations sur le calcul du nombre de demandes par seconde en provenance d'un serveur TIE, consultez la valeur **Débit** sous **Etat des performances** dans la page **Gestion de la topologie des serveurs TIE**, sous Paramètres serveur dans McAfee ePO. Vous pouvez également vous reporter à la valeur **Nouveaux fichiers de serveur TIE** dans la page **Nettoyage des données du serveur TIE**.

Configuration des paramètres TIE pour l'analyse des pièces jointes aux e-mails

Activez la vérification de la réputation TIE pour les pièces jointes aux e-mails en fonction de la catégorie de réputation des fichiers.

Procédure

1 Dans l'interface du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres TIE**.

2 Sélectionnez un élément dans la liste déroulante **Exécuter des actions si la réputation est égale ou inférieure à**.

- **Approuvé connu** : la réputation du fichier est de 99.
- **Très probablement approuvé** : la réputation du fichier est de 85.
- **Peut-être approuvé** : la réputation du fichier est de 70.
- **Inconnu** : la réputation du fichier est de 50.
- **Peut-être malveillant** : la réputation du fichier est de 30.

  L'option **Peut-être malveillant** est sélectionnée par défaut.

- **Très probablement malveillant** : la réputation du fichier est de 15.
- **Malveillant connu** : la réputation du fichier est de 1.

3 Dans **Entreprendre l'action suivante**, définissez les paramètres ci-dessous selon vos besoins.

- **Remplacer l'élément par une alerte** : remplace l'élément par un message d'alerte et journalise, met en quarantaine ou notifie selon l'option définie dans la section **Et aussi**.
- **Supprimer l'élément incorporé** : supprime la pièce jointe à l'e-mail et journalise, met en quarantaine ou notifie selon l'option définie dans la section **Et aussi**.
- **Supprimer le message** : supprime l'e-mail et journalise, met en quarantaine ou notifie selon l'option définie dans la section **Et aussi**.

4 Dans la section **Et aussi**, configurez les paramètres ci-dessous selon vos besoins.

- **Consigner**
- **Quarantaine**

- **Transférer l'e-mail mis en quarantaine**
- **Notifier l'administrateur**
- **Notifier l'expéditeur interne**
- **Avertir l'expéditeur externe**
- **Notifier le destinataire interne**
- **Avertir le destinataire externe**

5 Dans la section **Soumettre les fichiers à ATD si la réputation est égale ou inférieure à**, sélectionnez la catégorie et la taille de fichier pour la réputation Advanced Threat Defense.

Configuration des paramètres antispam

Configurez les paramètres dans une stratégie afin de détecter les e-mails de spam et d'entreprendre les actions nécessaires correspondantes.

Procédure

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

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 **Antispam**.

4 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de l'analyseur antispam 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.
- Si vous ajoutez un nouvel analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Dans la liste déroulante **Options**, sélectionnez un paramètre d'analyseur existant ou choisissez **<créer un nouveau jeu d'options>**.

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

6 Dans **Nom de l'instance**, tapez un nom unique pour l'instance de configuration de l'analyseur antispam. Ce champ est obligatoire.

7 Sous l'onglet **Options**, sous **Score**, tapez les valeurs pour les options suivantes :

- **Seuil de score élevé** : si le score de spam global est supérieur ou égal à 15.
- **Seuil de score moyen** : si le score de spam global est compris entre 10 et 15.
- **Seuil de score faible** : si le score de spam global est compris entre 5 et 10.

Pour utiliser les valeurs par défaut des scores de spam, sélectionnez l'option **Utiliser les valeurs par défaut**. Ces paramètres par défaut sont optimisés avec soin pour maintenir l'équilibre entre un taux de détection de spam élevé et un faible taux de faux positifs. Dans le cas peu probable où vous auriez besoin de modifier ces paramètres, un avis technique est disponible auprès du Support technique.

8 Dans **Rapports**, sous la liste déroulante **Le seuil de signalement des spams dans les rapports est**, sélectionnez **Elevé**, **Moyen**, **Faible** ou **Personnalisé** afin de spécifier le point auquel un message doit être marqué comme spam.

9 Dans **Score personnalisé**, tapez un score de spam spécifique auquel les e-mails doivent être marqués comme du spam. Ce champ est activé uniquement si vous sélectionnez l'option **Personnalisé** dans la liste déroulante **Le seuil de signalement des spams dans les rapports est**.

10 Sélectionnez ou désélectionnez **Ajouter un préfixe à l'objet des spams** le cas échéant.

11 Dans la liste déroulante **Ajouter un indicateur de score de spam**, sélectionnez :

- **Jamais** - Permet d'avoir l'en-tête Internet d'un message électronique sans indicateur de score de spam.
- **Aux spams uniquement** — Permet d'ajouter un indicateur de score de spam uniquement à l'en-tête Internet des messages électroniques de spam.
- **Aux non-spams uniquement** — Permet d'ajouter un indicateur de score de spam uniquement à l'en-tête Internet des messages électroniques de non-spam.
- **A tous les messages** — Permet d'ajouter un indicateur de score de spam uniquement à l'en-tête Internet de tous les e-mails.

L'indicateur de score de spam est un symbole utilisé dans le rapport de spam, ajouté dans l'en-tête Internet de l'e-mail afin d'indiquer la quantité de messages de spam potentiels contenue dans cet e-mail.

12 Dans la liste déroulante **Joindre un rapport de spam**, sélectionnez l'une des options suivantes :

- **Jamais** - Permet d'afficher un message électronique sans indicateur de score de spam.
- **Aux spams uniquement** — Permet d'ajouter un rapport de spam uniquement aux messages électroniques de spam.
- **Aux non-spams uniquement** — Permet d'ajouter un rapport de spam uniquement aux messages électroniques de non-spam.
- **A tous les messages** — Pour ajouter un rapport de spam à tous les e-mails.

13 Sélectionnez ou désélectionnez l'option **Rapport détaillé** afin de spécifier si un rapport détaillé est nécessaire ou non. Les rapports détaillés comprennent les noms des règles antispam qui ont été déclenchées, ainsi que leur description.

La sélection du paramètre **Jamais** pour l'option **Joindre un rapport de spam** entraîne la désactivation de l'option **Rapport détaillé**.

14 Sous l'onglet **Avancé**, utilisez les options suivantes :

- **Taille maximale des messages à analyser (Ko)** — Permet de spécifier la taille maximale (en kilo-octets) d'un e-mail pouvant être analysé. Vous pouvez saisir une taille atteignant 999 999 999 kilo-octets, bien que les messages de spam habituels soient de taille réduite. La valeur par défaut est 250 Ko.
- **Largeur maximale des en-têtes des spams (en octets)** — Permet de spécifier la taille maximale (en octets) que peut avoir l'en-tête du message de spam. La largeur d'en-tête minimale que vous pouvez spécifier est de 40 caractères et la largeur maximale est de 999 caractères. La valeur par défaut est 76.

  Les spammeurs ajoutent souvent des informations supplémentaires aux en-têtes pour leurs propres besoins.

- **Nombre maximal de règles signalées** — Permet de spécifier le nombre maximal de règles antispam pouvant être incluses dans un rapport de spam. Le nombre minimal de règles que vous pouvez spécifier est 1 et le maximal 999. La valeur par défaut est 180.
- **Nom de l'en-tête** — Permet de spécifier un autre nom pour l'en-tête de l'e-mail. Vous pouvez utiliser cet en-tête et sa valeur (ci-dessous) pour suivre les e-mails et leur appliquer des règles. Ces champs sont facultatifs et peuvent contenir jusqu'à 40 caractères.
- **Valeur de l'en-tête** — Permet de spécifier une autre valeur pour l'en-tête de l'e-mail.
- **Ajouter un en-tête** — Permet d'indiquer à quels e-mails l'en-tête doit être ajouté : aucun e-mail, tous les e-mails, uniquement les e-mails de spam ou les e-mails ne contenant pas de spam.
- Sélectionnez ou désélectionnez **Utiliser des noms d'en-têtes alternatifs lorsqu'un e-mail n'est pas du spam** le cas échéant.

15 Sous l'onglet **Listes de courrier**, sous **Expéditeurs bloqués**, **Expéditeurs autorisés**, **Destinataires bloqués** et **Destinataires autorisés**, indiquez les adresses e-mail des expéditeurs et destinataires bloqués et autorisés.

Les e-mails envoyés à ou depuis des adresses e-mail figurant dans une liste de blocage sont traités comme du spam, même s'ils ne présentent pas les caractéristiques du spam. Les e-mails envoyés à ou depuis des adresses e-mail figurant dans une liste d'autorisation ne sont pas traités comme du spam, même s'ils présentent les caractéristiques du spam.

Cliquez sur **Ajouter** pour ajouter des adresses à une liste et cochez la case en regard de chaque adresse afin de spécifier si elle est activée. Cliquez sur **Supprimer tout** pour supprimer une adresse e-mail de la liste. Vous ne pouvez pas ajouter la même adresse e-mail plusieurs fois. L'utilisation de caractères génériques vous permet de rechercher plusieurs adresses.

16 Dans l'onglet **Règles**, entrez le nom de la règle et sélectionnez **Activer la règle** pour l'activer. Cliquez sur **Ajouter** pour afficher une liste de règles disponibles.

Cliquez sur **Réinitialiser** pour retourner aux paramètres antispam par défaut.

17 Dans la liste, en regard de chaque règle, cliquez sur **Modifier** pour modifier la règle.

18 Cliquez sur **Supprimer** pour supprimer la règle.

19 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

20 Sous **Actions à entreprendre si un spam est détecté**, cliquez sur **Modifier**. Sous les onglets suivants, spécifiez les actions d'analyseur antispam devant être entreprises si un message de spam est détecté :

- **Score élevé**
- **Score moyen**
- **Score faible**

21 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

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

Procédures

- *Importation ou exportation de listes de blocage et de listes d'autorisation*, page 92
  Importez ou exportez des listes de blocage et des listes d'autorisation à des fins de sauvegarde ou d'utilisation sur un autre système Exchange Server.
- *Utilisation de la protection anti-usurpation*, page 93
  L'usurpation d'e-mails est une escroquerie fréquente consistant à capter les utilisateurs en modifiant l'adresse e-mail d'expéditeur, en les incitant à ouvrir l'e-mail et à y répondre, croyant qu'il provient d'une source légitime.
- *Configuration de la protection anti-usurpation*, page 93
  Activez la protection anti-usurpation pour protéger vos systèmes contre les e-mails d'usurpation.

Importation ou exportation de listes de blocage et de listes d'autorisation

Importez ou exportez des listes de blocage et des listes d'autorisation à des fins de sauvegarde ou d'utilisation sur un autre système Exchange Server.

Procédure

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

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 **Antispam**.

4 Sous **Options**, cliquez sur le lien **Bloquer une liste et autoriser une liste**.

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

5 Cliquez sur l'onglet **Listes de courrier**.

6 Sélectionnez la liste requise parmi les suivantes :

- **Expéditeurs bloqués**
- **Expéditeurs autorisés**
- **Destinataires bloqués**
- **Destinataires autorisés**

7 Pour importer une liste, cliquez sur **Importer**. Dans la fenêtre pop-up, cliquez sur **Parcourir** pour accéder au fichier `.cfg` requis, puis cliquez sur **OK**.

8 Pour exporter une liste, cliquez sur le lien **Exporter**.

Cliquez sur **Supprimer** pour supprimer une liste de la base de données.

9 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

Utilisation de la protection anti-usurpation

L'usurpation d'e-mails est une escroquerie fréquente consistant à capter les utilisateurs en modifiant l'adresse e-mail d'expéditeur, en les incitant à ouvrir l'e-mail et à y répondre, croyant qu'il provient d'une source légitime.

MSME prend désormais en charge une fonction d'anti-usurpation reposant sur le mécanisme Sender Policy Framework (SPF) de l'IETF (Internet Engineering Task Force). La structure SPF repose sur la norme RFC 7208 qui autorise l'utilisation de noms de domaine dans les e-mails.

Le résultat est catégorisé comme suit d'après l'évaluation SPF du domaine d'expéditeur :

- Aucun
- Neutre
- Réussite
- Echec ou Erreur matérielle
- Erreur logicielle
- Erreur temporaire
- Erreur permanente

L'option Filtre SPF permet de configurer les actions à réaliser en cas d'erreur logicielle ou matérielle. Afin de réduire les faux positifs, MSME considère les catégories restantes comme réussies. Lorsque SPF est activé, vous pouvez visualiser le résultat SPF dans l'en-tête de l'e-mail **Received-SPF**.

Configuration de la protection anti-usurpation

Activez la protection anti-usurpation pour protéger vos systèmes contre les e-mails d'usurpation.

Avant de commencer

Vous devez avoir installé le composant McAfee Anti-Spam sur le serveur Exchange.

Procédure

1. Sélectionnez **Paramètres et diagnostics** | **Antispam**
2. Dans la section **Filtre SPF**, sélectionnez **Activer**.
3. Configurez l'action requise pour **Erreur matérielle** et **Erreur logicielle**.
   - **Autoriser** : autorise l'acheminement de l'e-mail jusqu'à son destinataire.
   - **Autoriser le transfert et mettre en quarantaine** : autorise l'acheminement de l'e-mail jusqu'à son destinataire et en conserve une copie dans la section des éléments mis en quarantaine.
   - **Rejeter l'e-mail et mettre en quarantaine** : bloque l'e-mail et le met en quarantaine.

   L'activation de cette option peut réduire les performances du produit dans la mesure où la protection anti-usurpation interroge les serveurs DNS et est dépendante de la latence réseau.

Configuration des paramètres antiphishing

Configurez les paramètres dans une stratégie afin de bloquer les messages de phishing (hameçonnage) à l'aide du moteur et des règles antispam et d'entreprendre les actions nécessaires.

Procédure

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

   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 **Antihameçonnage**.

4 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de l'analyseur antiphishing (antihameçonnage) 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.
- Si vous ajoutez un nouvel analyseur à la stratégie, vous pouvez spécifier une plage horaire d'activation de l'analyseur à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Dans la liste déroulante **Options**, sélectionnez un paramètre d'analyseur existant ou choisissez **<créer un nouveau jeu d'options>**.

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

6 Sous **Nom de l'instance**, saisissez un nom unique pour l'instance de paramètre de l'analyseur antiphishing (antihameçonnage). Ce champ est obligatoire.

7 Sous **Options de rapport**, sélectionnez ou désélectionnez les options suivantes comme il convient :

- **Ajouter un préfixe à l'objet des messages de phishing** : spécifie que vous souhaitez ajouter du texte au début de la ligne d'objet de tout e-mail susceptible de contenir des informations de phishing.
- **Ajouter un en-tête indicateur de phishing aux messages** : spécifie qu'un indicateur de phishing doit être ajouté ou non à l'en-tête Internet des e-mails susceptibles de contenir des informations de phishing.
- **Joindre un rapport des messages de phishing** : spécifie qu'un rapport des messages de phishing doit être généré et ajouté à tout e-mail détecté comme message de phishing.
- **Rapport détaillé** : spécifie que les noms des règles antiphishing déclenchées ainsi que leur description détaillée doivent être inclus dans l'e-mail. Cette option est uniquement disponible si vous avez sélectionné **Joindre un rapport des messages de phishing**.

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

9 Dans **Actions à entreprendre**, cliquez sur **Modifier** et spécifiez les actions antiphishing que l'analyseur doit entreprendre si un message de phishing est détecté.

10 Cliquez sur **Enregistrer** pour appliquer les paramètres et revenir à la page des paramètres de stratégie.

11 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**
- **Filtrage selon la taille du courrier**
- **Contrôle de l'analyseur**
- **Paramètres du courrier MIME**

- **Contenu signé**
- **Fichiers protégés par mot de passe**
- **Fichiers HTML**

Procédures

- *Configuration des paramètres de contenu corrompu*, page 95
  Configurez les paramètres dans une stratégie afin d'identifier les e-mails au contenu corrompu et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de contenu protégé*, page 96
  Configurez les paramètres dans une stratégie afin d'identifier les e-mails au contenu protégé et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de contenu chiffré*, page 96
  Configurez les paramètres dans une stratégie afin d'identifier les e-mails au contenu chiffré et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de contenu signé*, page 97
  Configurez les paramètres dans une stratégie afin d'identifier les e-mails au contenu signé et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de fichiers protégés par mot de passe*, page 98
  Configurez les paramètres dans une stratégie afin d'identifier les e-mails aux archives protégées par mot de passe et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de filtrage de taille d'e-mail*, page 98
  Paramètres de filtrage de taille d'e-mail dans une stratégie basée sur leur taille, du nombre de pièces jointes et de la taille des pièces jointes.
- *Configuration des paramètres de contrôle de l'analyseur*, page 99
  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 d'un e-mail.
- *Blocage manuel des adresses IP*, page 100
  Vous pouvez bloquer une adresse IP spécifique ou une plage d'adresses IP afin d'empêcher l'envoi d'e-mails à votre organisation à partir de cette ou de ces adresses IP, indépendamment de leur réputation. Pour activer cette option, vous devez mettre à jour le registre suivant.
- *Configuration des paramètres d'e-mail MIME*, page 101
  Configurez les paramètres dans une stratégie afin d'identifier les messages MIME codés et d'entreprendre les actions nécessaires correspondantes.
- *Configuration des paramètres de fichiers HTML*, page 103
  Configurez les paramètres dans une stratégie afin de rechercher des éléments ou de supprimer des exécutables tels que des contrôles ActiveX, des applets Java et des scripts VBScript dans des composants HTML d'un e-mail.

Configuration des paramètres de contenu corrompu

Configurez les paramètres dans une stratégie afin d'identifier les e-mails au contenu corrompu et d'entreprendre les actions nécessaires correspondantes.

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

Procédure

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**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

4 Dans **Actions**, cliquez sur **Modifier** pour indiquer les actions de filtre qui doivent être entreprises lors de la détection de contenu corrompu.

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

6 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 e-mails au contenu protégé et d'entreprendre les actions nécessaires correspondantes.

Les stratégies de contenu protégé déterminent le mode de traitement des e-mails en cas de détection d'un contenu protégé.

Procédure

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**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

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

5 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

6 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 e-mails au contenu chiffré et d'entreprendre les actions nécessaires correspondantes.

Vous avez la possibilité de chiffrer les e-mails afin d'empêcher les parties non autorisées d'y accéder. Un contenu chiffré fait appel à une *clé* et à des algorithmes mathématiques de chiffrement destinés à déchiffrer celle-ci. Les stratégies de contenu chiffré déterminent le mode de gestion des e-mails chiffrés lors de leur détection.

Procédure

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**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

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

5 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

Les paramètres Contenu crypté s'appliquent aux pièces jointes chiffrées des e-mails internes et aux e-mails chiffrés d'Internet.

6 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 e-mails au contenu signé et d'entreprendre les actions nécessaires correspondantes.

Lorsque vous envoyez des informations par voie électronique, elles risquent d'être altérées, accidentellement ou délibérément. Pour remédier à ce problème, certains logiciels de messagerie ont donc recours à des signatures numériques, forme électronique d'une signature manuscrite.

Une signature numérique consiste en des données supplémentaires ajoutées à un message, qui identifient et authentifient l'expéditeur, de même que les informations contenues dans le message. Elle est cryptée et joue en quelque sorte le rôle de résumé unique des données transmises. En règle générale, il s'agit d'une longue chaîne de lettres et de chiffres qui figure au bas d'un message reçu. Le logiciel de messagerie réexamine les informations du message de l'expéditeur et crée une signature numérique. Si la signature est identique à celle d'origine, cela signifie que les données n'ont pas été modifiées.

Si l'e-mail 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. L'e-mail est toujours valide et accessible en lecture, mais la signature numérique d'origine est « cassée ». Le destinataire ne peut pas se fier au contenu du message, car celui-ci a peut-être été altéré d'autres façons. Les stratégies de gestion du contenu signé indiquent de quelle manière les e-mails contenant des signatures numériques doivent être traités une fois détectés.

Procédure

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**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

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

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

Les paramètres de contenu signé s'appliquent aux e-mails et aux pièces jointes signés.

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

Configuration des paramètres de fichiers protégés par mot de passe

Configurez les paramètres dans une stratégie afin d'identifier les e-mails aux archives protégées par mot de passe et d'entreprendre les actions nécessaires correspondantes.
Il est impossible d'accéder aux fichiers protégés par mot de passe et d'analyser la présence de logiciels malveillants sans mot de passe. Des stratégies spécifient comment traiter les e-mails qui contiennent un fichier protégé par mot de passe.

Procédure

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 **Fichiers protégés par mot de passe**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

4 Dans **Actions**, cliquez sur **Modifier** pour spécifier les actions de filtre qui doivent être entreprises lors de la détection d'un e-mail contenant un fichier protégé par mot de passe.

Si vous définissez l'action comme **Autoriser**, assurez-vous que la **Règle de contournement protégée par mot de passe** sous **Règles de filtrage de fichiers et actions associées** dans les paramètres de l'analyseur **Filtrage des fichiers** est la première règle de la liste. Si la règle est déjà répertoriée à un niveau différent, supprimez la règle, puis sélectionnez la règle à partir de la liste déroulante **Règles disponibles**.

5 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

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

Configuration des paramètres de filtrage de taille d'e-mail

Paramètres de filtrage de taille d'e-mail dans une stratégie basée sur leur taille, du nombre de pièces jointes et de la taille des pièces jointes.

Avant de commencer
Assurez-vous que sur la page **Paramètres à l'accès**, les options **Analyser les e-mails entrants** et **Analyser les e-mails sortants** sont sélectionnées.

Vous pouvez configurer séparément les paramètres de filtrage de taille d'e-mail pour la stratégie **Passerelle** et la stratégie **A l'accès**. Configurez les paramètres **Passerelle** pour les e-mails entrants et les paramètres **A l'accès** pour les e-mails sortants. Par exemple :

- Pour bloquer tous les e-mails entrants contenant plus de cinq pièces jointes, configurez les paramètres **Filtrage de taille d'e-mail** pour la stratégie **Passerelle**.
- Pour bloquer tous les e-mails sortants contenant plus de trois pièces jointes, configurez les paramètres **Filtrage de taille d'e-mail** pour la stratégie **A l'accès**.

Le filtrage de taille d'e-mail pour l'analyse à l'accès n'est pas applicable pour le rôle de serveur de boîte aux lettres.

Procédure

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 Sélectionnez la stratégie comme requis pour la stratégie **A l'accès** ou **Passerelle** :

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

4 Cliquez sur **Filtrage selon la taille du courrier**.

5 Sous **Activation**, sélectionnez **Activer** pour activer les paramètres de filtre de taille d'e-mail correspondant à l'élément de sous-menu choisi.

> Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

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

- **Paramètres par défaut** — Permet d'afficher une synthèse du jeu d'options de taille de courrier utilisé par défaut.
- **Paramètres de passerelle par défaut** — Permet d'afficher une synthèse de l'option de taille de l'e-mail par défaut utilisée par la stratégie de passerelle.
- **<create new set of options>** — Permet de configurer des options de filtrage de taille d'e-mail. Les options sont les suivantes :
  - **Nom de l'instance** — Tapez un nom unique l'instance de configuration du filtre de taille d'e-mail. Ce champ est obligatoire.
  - **Taille maximale totale du courrier (Ko)** — Permet de spécifier la taille maximale (en kilo-octets) d'un e-mail. Vous pouvez indiquer une valeur comprise entre 2 Ko et 2 Go, la valeur par défaut étant 20 000 Ko.
  - **Taille maximale des pièces jointes (Ko)** — Permet de spécifier la taille maximale (en kilo-octets) des pièces jointes d'un e-mail. Vous pouvez indiquer une valeur comprise entre 1 Ko et 2 Go, la valeur par défaut étant 4 096 Ko.
  - **Nombre maximal de pièces jointes** — Permet de spécifier le nombre maximal de pièces jointes pouvant être ajoutées à un e-mail. Vous pouvez indiquer une valeur jusqu'à 999, la valeur par défaut étant 25.
- **Modifier** — Permet de modifier le jeu d'options sélectionné.

7 Sous **Actions**, cliquez sur **Modifier**. Spécifiez les actions de filtre de taille d'e-mail à entreprendre si la valeur dépasse les paramètres spécifiés pour ces options :

- **Taille du message**
- **Taille de la pièce jointe**
- **Nombre de pièces jointes**

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

> Les e-mails internes ne sont pas détectés par les règles de filtrage de taille d'e-mail.

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 d'un e-mail.

Procédure

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**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

4 Dans **Options**, cliquez sur **<créer un nouveau jeu d'options>**.

5 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.

6 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 10.

7 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 10.

8 Dans le champ **Durée maximale d'analyse (minutes)**, spécifiez la durée maximale autorisée pour l'analyse d'un fichier. Vous pouvez indiquer une valeur comprise entre 1 et 999, la valeur par défaut étant 1.

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 Sous **Actions**, cliquez sur **Modifier** afin de spécifier les actions à entreprendre si la valeur dépasse les paramètres spécifiés pour ces options :

- **Niveau maximal d'imbrication**
- **Taille maximale du fichier décompressé (Mo)**
- **Durée maximale d'analyse (minutes)**

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

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

Blocage manuel des adresses IP

Vous pouvez bloquer une adresse IP spécifique ou une plage d'adresses IP afin d'empêcher l'envoi d'e-mails à votre organisation à partir de cette ou de ces adresses IP, indépendamment de leur réputation. Pour activer cette option, vous devez mettre à jour le registre suivant.

Avant de commencer

Le blocage manuel des adresses IP est possible uniquement au niveau des rôles Exchange, Hub, Edge, MailBox et HubMB. La fonction de détection de McAfee Anti-Spam doit être disponible dans MSME pour que vous puissiez ajouter manuellement des adresses IP dans une liste noire.

Procédure

1 Sur le système doté de MSME, accédez à la clé de registre suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState`

2 Ajoutez la valeur de chaîne `IPBlackList`.

3 Affectez l'adresse IPv4 pour laquelle vous souhaitez bloquer l'envoi d'e-mails.

Pour bloquer plusieurs adresses IP, séparez-les au moyen d'un point-virgule. Vous pouvez également bloquer une plage d'adresses IP à l'aide du caractère générique `*`. Exemple :

- `10.21.22.*` : bloque toutes les adresses IP comprises entre `10.21.22.0` et `10.21.22.255`
- `10.21.*.*` : bloque toutes les adresses IP comprises entre `10.21.0.1` et `10.21.255.255`.

Configuration des paramètres d'e-mail MIME

Configurez les paramètres dans une stratégie afin d'identifier les messages MIME codés et d'entreprendre les actions nécessaires correspondantes.

MIME (Multipurpose Internet Mail Extensions) est un standard de communication qui permet le transfert de formats non-ASCII via des protocoles (tels SMTP) prenant uniquement en charge 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.

Procédure

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 **Paramètres du e-mail MIME**.

Si vous ajoutez un nouveau filtre à la stratégie, vous pouvez spécifier une plage horaire d'activation du filtre à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

4 Sous **Options**, sélectionnez **<créer un nouveau jeu d'options>**.

La page **Paramètres du courrier** s'affiche.

5 Dans **Nom de l'instance**, tapez un nom unique pour l'instance de configuration du filtre de e-mail MIME. Ce champ est obligatoire.

6 Sous l'onglet **Options**, renseignez le champ **Préfixe de l'objet du message**.

a Dans **Nouvel encodage par défaut des pièces jointes dans un message MIME**, sélectionnez une méthode de codage utilisée lors du nouvel encodage des pièces jointes du e-mail MIME dans les options disponibles.

b Dans **Nouvel encodage par défaut des pièces jointes dans un message MIME**, sélectionnez une méthode de codage utilisée lors du nouvel encodage des en-têtes d'objets du e-mail MIME dans les options disponibles.

c Dans **Si le recodage d'un en-tête d'objet échoue**, sélectionnez une de ces options :

- **Considérer comme une erreur —** Le message MIME est retourné.
- **Revenir en UTF-8 —** Le message MIME est codé en UTF-8.

7 Sous l'onglet **Avancé**, sélectionnez l'une de ces méthodes de codage pour l'utiliser lors du codage de la partie textuelle d'un e-mail :

- **Quoted-Printable**, qui est plus adapté pour les messages qui contiennent principalement des caractères ASCII, mais qui contient également certaines valeurs d'octets hors de la plage.
- **Base64**, dont les ressources nécessaires au traitement sont fixes et qui est particulièrement adaptée aux données non textuelles et aux messages qui ne contiennent que peu de texte ASCII.
- **8 bits**, méthode particulièrement adaptée aux serveurs SMTP prenant en charge l'extension de transport SMTP 8BIT MIME.

> Vous pouvez uniquement effectuer l'*étape 6b* si vous sélectionnez **Re-coder à l'aide du schéma de codage d'origine** ou **Re-coder avec le jeu de caractères suivant** depuis **Recodage à privilégier pour les en-têtes d'objet modifiés**.

a Sélectionnez ou désélectionnez **Ne pas encoder le texte en 7 bits** le cas échéant.

b Dans **Jeu de caractères par défaut pour le décodage**, sélectionnez un jeu de caractères à utiliser pour le décodage lorsqu'aucun jeu n'est spécifié par les en-têtes MIME.

c Dans **Nombre maximal de parties MIME**, spécifiez le nombre maximal de parties MIME que peut contenir un message MIME. La valeur par défaut est 10 000 parties MIME.

d Dans **Altération d'en-tête dans un message MIME**, sélectionnez l'option adéquate.

e Dans **Caractères NULL dans les en-têtes de message MIME**, sélectionnez l'option adéquate.

f Dans **Altération d'en-tête dans un message MIME**, sélectionnez l'option adéquate.

8 Dans l'onglet **Types MIME**, spécifiez les types MIME à traiter comme étant des pièces jointes textuelles et ceux à considérer comme étant des pièces jointes binaires.

> Cliquez sur **Ajouter** pour ajouter les types MIME à la liste ou **Supprimer** pour supprimer un type MIME d'une liste. Les entrées en double ne sont pas autorisées.

9 Sous l'onglet **Jeux de caractères**, sélectionnez **Jeu de caractères** et **Alternatives**, désactivez la case à cocher **Fixe**, puis cliquez sur **Ajouter** pour indiquer un mappage de jeu de caractères de remplacement pour le jeu spécifié dans le message MIME.

> Cliquez sur **Modifier** pour corriger les mises en correspondance de jeux de caractères, sur **Supprimer** pour supprimer ces mises en correspondance et sur **Enregistrer** pour enregistrer toutes les modifications apportées aux mises en correspondance.
>
> L'option **Enregistrer** est disponible seulement quand vous cliquez sur **Modifier**.

10 Cliquez sur **Enregistrer**.

11 Sous **Sélection d'alerte**, vous pouvez sélectionner l'alerte à utiliser lorsqu'un message de type MIME est bloqué. 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.

12 Dans **Actions de message incomplet**, cliquez sur **Modifier**pour spécifier les actions de filtre qui doivent être entreprises lors de la détection d'un MIME partiel ou d'un type MIME externe.

13 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

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

Configuration des paramètres de fichiers HTML

Configurez les paramètres dans une stratégie afin de rechercher des éléments ou de supprimer des exécutables tels que des contrôles ActiveX, des applets Java et des scripts VBScript dans des composants HTML d'un e-mail.

Si un de ces types de HTML est détecté dans le contenu, il est supprimé. Ce filtre fonctionne seulement si Analyseur de contenu est activé.

Procédure

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 **Fichiers HTML**.

4 Sous **Options**, cliquez sur **<créer un nouveau jeu d'options>**.

La page **Fichiers HTML** s'affiche.

5 Sous **Nom de l'instance**, saisissez un nom unique pour l'instance du paramètre de filtre. Ce champ est obligatoire.

6 Sous **Analyser les éléments suivants**, sélectionnez l'une de ces options :

- **Commentaires** — Permet d'analyser les éléments de commentaires du message HTML. Exemple :

```
<!-- texte de commentaire --!>
```

- **Métadonnées** — Permet d'analyser les éléments de métadonnées du message HTML. Par exemple :

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- **URL sous forme de liens ("<ahref=...")** — Permet d'analyser les URL du message HTML. Exemple :

```
<a HREF="McAfee.htm">
```

- **URL sources ("<img src=...")** — Permet d'analyser les URL sources du message HTML. Exemple :

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- **Javascript/VBScript** — Permet d'analyser les éléments de script JavaScript ou Visual Basic du message HTML. Exemple :

```
<script language="javascript" scr="mfe/mfe.js">
```

7 Sous **Supprimer les éléments exécutables suivants**, sélectionnez l'une de ces options :

- **Javascript/VBScript** — Permet de supprimer les éléments de script JavaScript ou Visual Basic du message HTML. Exemple :

```
<script language="javascript" scr="mfe/mfe.js">
```

- **Applets Java** — Permet de supprimer les éléments d'applets Java du message HTML. Exemple :

```
<APPLET code="XYZApp.class" codebase="HTML ....."></APPLET>
```

- **Contrôles ActiveX** — Permet de supprimer les éléments de contrôles ActiveX du message HTML. Exemple :

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan
Image </OBJECT>
```

- **Macromedia Flash** — Permet de supprimer les éléments Macromedia Flash du message HTML. Cette option est activée si vous avez sélectionné Contrôles ActiveX. Exemple :

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

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

Gestion de divers paramètres associés à une stratégie

Créez ou modifiez divers paramètres (tels que les alertes et les clauses d'exclusion de responsabilité) appliqués suite au déclenchement d'une stratégie.

Les options disponibles sont les suivantes :

- **Paramètres d'alerte**
- **Texte d'avis de non-responsabilité**

Procédures

- *Configuration des paramètres des messages d'alerte*, page 104
  Configurez les paramètres dans une stratégie afin de prévenir l'utilisateur final de la survenue d'une détection par un message d'alerte.
- *Configuration des paramètres du texte de la clause d'exclusion de responsabilité*, page 106
  Configurez dans une stratégie les paramètres du texte de la clause d'exclusion de responsabilité, laquelle correspond généralement à une mention légale, qui est ajoutée à tous les e-mails sortants.

Configuration des paramètres des messages d'alerte

Configurez les paramètres dans une stratégie afin de prévenir l'utilisateur final de la survenue d'une détection par un message d'alerte.

Procédure

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 **Paramètres d'alerte**.

4 Sélectionnez **Activer** pour activer les paramètres du message d'alerte 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.
- Si vous ajoutez un nouveau paramètre de message d'alerte à la stratégie, vous pouvez spécifier une plage horaire d'activation à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Sous **Options**, sélectionnez les paramètres d'alerte par défaut disponibles ou choisissez **<créer un nouveau jeu d'options>** pour définir vos paramètres d'alerte.

Pour des instructions détaillées sur la procédure de création d'une alerte, consultez la section *Création d'une nouvelle alerte*.

6 Cliquez sur **Modifier** pour modifier une alerte existante.

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

7 Sélectionnez **HTML** ou **Texte brut** comme **Format de l'alerte**.

8 Dans le menu déroulant **Codage des caractères**, sélectionnez un jeu de caractères requis.

9 Dans **Nom de fichier de l'alerte**, spécifiez le nom du fichier pour cette alerte, y compris l'extension de fichier correspondante, HTML (.htm) ou texte brut (.txt).

10 Sélectionnez ou désélectionnez **Activer les en-têtes des alertes** pour activer l'utilisation d'un en-tête d'alerte.

11 Dans la zone de saisie de texte **En-tête de l'alerte**, tapez l'en-tête pour l'alerte.

12 Dans **Afficher**, sélectionnez **Contenu HTML (WYSIWYG)** ou **Contenu HTML (source)** selon si le texte HTML doit être affiché sous la forme de code compilé ou code source dans l'**En-tête de l'alerte**.

L'option **Afficher** est disponible uniquement si vous avez sélectionné **HTML** comme format de message d'alerte.

13 Sélectionnez **Activer les pieds de page des alertes** pour activer l'utilisation d'un pied de page d'alerte le cas échéant.

14 Dans la zone de saisie de texte **Pied de page de l'alerte**, tapez le pied de page pour l'alerte.

15 Dans **Afficher**, sélectionnez **Contenu HTML (WYSIWYG)** ou **Contenu HTML (source)** selon si le texte HTML doit être affiché sous la forme de code compilé ou code source dans le **Pied de page de l'alerte**.

L'option **Afficher** est disponible uniquement si vous avez sélectionné **HTML** comme format de message d'alerte.

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

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

Configuration des paramètres du texte de la clause d'exclusion de responsabilité

Configurez dans une stratégie les paramètres du texte de la clause d'exclusion de responsabilité, laquelle correspond généralement à une mention légale, qui est ajoutée à tous les e-mails sortants.

S'ils sont affectés à une stratégie, tous les e-mails quittant l'organisation Exchange via le serveur MSME se verront appliquer le texte de la clause d'exclusion de responsabilité en fonction des paramètres configurés.

Les paramètres du texte de la clause d'exclusion de responsabilité concernent uniquement les serveurs Microsoft Exchange Transport.

Procédure

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 **Texte d'avis de non-responsabilité**.

4 Sélectionnez **Activer** pour activer les paramètres du texte de la clause d'exclusion de responsabilité 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.
- Si vous ajoutez un nouveau paramètre de texte de clause d'exclusion de responsabilité à la stratégie, vous pouvez spécifier une plage horaire d'activation à partir de la liste déroulante **A quelle heure souhaitez-vous que ceci s'applique ?**.

5 Dans **Options**, sélectionnez**<créer un nouveau jeu d'options>**. La page **Texte d'avis de non-responsabilité** s'affiche.

6 Dans **Nom de l'instance**, tapez un nom unique pour l'instance de configuration du texte de clause d'exclusion de responsabilité. Ce champ est obligatoire.

7 Sous Format de la clause d'exclusion de responsabilité, vous pouvez sélectionner les options suivantes :

- **HTML** : permet de spécifier que la clause d'exclusion de responsabilité doit s'afficher au format HTML dans l'e-mail de notification.
- **Texte brut** : permet de spécifier que la clause d'exclusion de responsabilité doit s'afficher au format texte simple dans l'e-mail de notification.

8 Dans la zone de texte **Modifier le contenu de la clause d'exclusion de responsabilité**, saisissez le texte de la clause.

9 Sous **Afficher**, sélectionnez **Contenu HTML (WYSIWYG)** ou **Contenu HTML (source)** selon que le texte HTML doit s'afficher sous forme de code compilé ou de code source dans la zone **Pied de page de l'alerte**.

L'option **Afficher** est uniquement disponible si vous avez sélectionné **HTML** comme format de texte pour la clause d'exclusion de responsabilité.

10 Dans la liste déroulante **Insérer la clause d'exclusion de responsabilité**, sélectionnez **Avant le texte du message**, **Après le texte du message** ou **Comme pièce jointe au message** selon l'emplacement du texte de la clause d'exclusion de responsabilité dans l'e-mail et la méthode d'insertion employée.

11 Cliquez sur **Enregistrer** pour retourner à la page de stratégie.

Les clauses d'exclusion de responsabilité s'appliquent uniquement aux e-mails sortants.

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

5 Paramètres et diagnostics

La page **Paramètres et diagnostics** dispose de menus destinés à l'activation, la désactivation, la configuration et l'administration des fonctionnalités de MSME, ainsi qu'aux journaux associés. Configurez ces paramètres en fonction des stratégies de sécurité de votre organisation.

Pour modifier ou afficher les paramètres du produit MSME, 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 5-1 Paramètres et diagnostics

Paramètres	Objectif
Paramètres à l'accès Les **Paramètres à l'accès** sont disponibles uniquement sur les serveurs Microsoft Exchange Server 2010. La prise en charge de Microsoft VSAPI n'étant plus assurée dans Microsoft Exchange 2013 et 2016, les fonctionnalités Paramètres VSAPI à l'accès et Paramètres de l'analyse en arrière-plan sont désactivées pour Exchange Server 2013 et 2016.	Décidez de ce qu'il advient d'un e-mail en cas d'échec de l'analyse. Les options sont les suivantes : • **Autoriser** • **Supprimer** Le menu comprend des sous-menus permettant d'activer ou de désactiver les paramètres suivants : • **API d'analyse antivirus de Microsoft (VSAPI)** • **Paramètres de l'analyse en arrière-plan** • **Paramètres d'analyse du trafic**
Paramètres à la demande	Modifiez le mot de passe pour l'utilisateur **MSMEODUser** et pour synchroniser la mise à jour du mot de passe avec l'Active Directory et les autres serveurs Exchange.
Paramètres d'exclusion de la boîte aux lettres	Définissez les boîtes aux lettres, dossiers et sous-dossiers à exclure de l'analyse VSAPI à l'accès.
Notifications	• Définissez un compte de messagerie administrateur auquel les notifications seront adressées ou envoyez des e-mails de notification à des réviseurs précis ou à des listes de distribution suite à la détection d'un e-mail. • Créez des e-mails de notification personnalisés qui sont envoyés aux utilisateurs suite à la mise en quarantaine d'un e-mail. • Définissez des alertes relatives à l'intégrité des produits qui sont envoyées par e-mail à l'administrateur une fois par jour ou dès qu'un événement donné se produit (par ex. problème avec la base de données Postgres ou échec du chargement d'un service).

Tableau 5-1 Paramètres et diagnostics *(suite)*

Paramètres	Objectif
Antispam	• Définissez les paramètres du dossier de courrier indésirable vers lequel le spam détecté sur un serveur de transport Edge (Passerelle) doit être transféré. • Activez ou désactivez la fonctionnalité **Réputation des messages McAfee GTI**. • Activez ou désactivez la fonctionnalité **Filtre SPF**. • Activez ou désactivez la fonctionnalité **Réputation des adresses IP McAfee GTI**.

Paramètres TIE	Configurez et gérez les paramètres de détection TIE ci-après :
	• **Exécuter des actions si la réputation est égale ou inférieure à** : autorise l'action lorsque le score de réputation est inférieur ou égal au seuil défini.
	• **Entreprendre l'action suivante**
	  • **Remplacer l'élément par une alerte**
	  • **Supprimer l'élément incorporé**
	  • **Supprimer le message**
	  • **Et aussi** : propose plusieurs options, notamment de journalisation, de mise en quarantaine ou de notification.
	• **Soumettre les fichiers à ATD si la réputation est égale ou inférieure à** et **Limiter la taille des fichiers à** : permettent d'envoyer des fichiers pour vérification de la réputation Advanced Threat Defense avec correspondance du seuil de réputation TIE et de la limite de taille de fichier.

Eléments détectés	Configurez et gérez les référentiels de quarantaine à l'aide de l'une des options suivantes : • **McAfee Quarantine Manager** : permet de configurer les paramètres de communication entre MSME et le serveur MQM (le cas échéant). • **Base de données locale** : permet de gérer et d'administrer les activités de la base de données de quarantaine locale comme la purge et l'optimisation.
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 aux journaux du produit et aux événements de débogage, notamment les informations sur la taille et l'emplacement d'enregistrement des journaux. Les paramètres de diagnostics sont les suivants : • **Journalisation de débogage** • **Journalisation des événements** • **Journal du produit** • **Service de notification d'erreurs**
Journal du produit	Permet de consulter le **Journal du produit** et de filtrer la sortie par date, type ou description.
Paramètres de DAT	Conservez les fichiers DAT précédents au lieu de les écraser avec chaque nouvelle mise à jour et définissez le nombre de fichiers de définition de détection à conserver.

Tableau 5-1 Paramètres et diagnostics *(suite)*

Paramètres	Objectif
Importer et exporter la configuration	Configurez votre serveur MSME actuel avec les mêmes configurations que celle qui est déjà créée, restaurez les paramètres par défaut ou les paramètres améliorés, ou créez des fichiers Sitelist pointant vers les sites de téléchargement des fichiers DAT.
Paramètres de proxy	Configurez ou modifiez les paramètres de proxy du service **Programme de mise à jour des règles antispam McAfee**.

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.
- vert si vous n'avez pas modifié de paramètre existant ou que la modification est appliquée.

Sommaire

Paramètres à l'accès

L'analyse à l'accès est déclenchée au niveau de la passerelle ou chaque fois que des utilisateurs accèdent à des e-mails, afin de déterminer si un élément est détecté par la stratégie correspondante. L'analyse à l'accès est également appelée analyse en temps réel.

Chaque analyse possède des avantages propres suivant le rôle serveur Exchange dans lequel MSME est installé. Le tableau ci-dessous permet de mieux comprendre les types d'analyse, les fonctions associées et les situations où chaque analyse est applicable :

Rôle Exchange Server	Stratégies applicables	Type d'analyse	Description
Transport Edge ou transport Hub	• A l'accès • Passerelle	Analyse du trafic à l'accès	Recherche les menaces avant que l'e-mail n'atteigne le serveur de boîtes aux lettres. En activant cette option, MSME peut détecter les menaces au niveau du périmètre de votre organisation et ainsi réduire la charge du serveur de boîtes aux lettres.
Boîte aux lettres	• A l'accès	Analyse VSAPI à l'accès	Recherche les menaces lorsqu'un utilisateur accède à un e-mail à l'aide d'un client de messagerie tel qu'Outlook.

Rôle Exchange Server	Stratégies applicables	Type d'analyse	Description
		Analyse proactive	Recherche les menaces avant qu'un e-mail ne soit écrit dans la banque d'informations Microsoft Exchange.
		Analyse de la boîte d'envoi	Recherche les menaces présentes dans un e-mail situé dans le dossier Boîte d'envoi.
		Analyse en arrière-plan	Analyse de priorité faible qui recherche en arrière-plan les menaces présentes dans toutes les bases de données Exchange.

A partir de la section **Général**, définissez une action à entreprendre en cas d'échec d'une analyse.

Un échec de l'analyse peut survenir pour l'une de ces raisons :

- **Lors d'une panne générale —** L'analyseur ne peut pas analyser un fichier en particulier.
- **Lors d'une panne du produit —** L'analyse ne fonctionne pas du fait d'un fichier DAT ou d'un moteur erroné, ou de règles antispam erronées.

Il peut s'agir de problèmes techniques tels que les suivants :

- Expiration de l'analyse
- Echec du chargement du moteur d'analyse
- Problèmes relatifs aux fichiers DAT
- E-mails formatés de manière incorrecte

Par exemple, une analyse peut se solder par un échec en cas de non-concordance de fichiers DAT entre le Registre et l'emplacement réel (`\bin\DATs`).

Dans le cas d'une panne d'analyse, une action est déclenchée en fonction des paramètres spécifiés sous **Paramètres et diagnostics | Paramètres à l'accès | Général**.

Tableau 5-2 Définition des options

Option	Définition
En cas d'échec de l'analyse générale	• **Autoriser** : autorise l'acheminement de l'e-mail jusqu'au destinataire visé en cas d'échec de l'analyse. • **Supprimer** : supprime l'e-mail en cas d'échec de l'analyse.
En cas d'échec de l'analyse du produit	• **Autoriser** : autorise l'acheminement de l'e-mail jusqu'au destinataire visé en cas d'échec de l'analyse. • **Supprimer** : supprime l'e-mail en cas d'échec de l'analyse.

McAfee recommande de toujours définir cette option sur **Autoriser** afin d'éviter que des e-mails légitimes soient mis en quarantaine suite à l'échec d'une analyse. Par défaut, le paramètre **Autoriser** est attribué par cette option afin d'éviter la perte d'e-mails en cas d'échec d'une analyse.

Les autres catégories disponibles sur la page **Paramètres à l'accès** sont les suivantes :

- **API d'analyse antivirus de Microsoft (VSAPI)**
- **Paramètres de l'analyse en arrière-plan**
- **Paramètres d'analyse du trafic**

Dans la section Paramètres d'analyse du trafic, vous pouvez exclure de l'analyse les e-mails possédant la taille définie. Par défaut, les fichiers de 4 Mo sont exclus.

Pour plus d'informations sur les types d'analyses, consultez l'article KB51129 dans la base de connaissances McAfee KnowledgeBase.

Paramètres de Microsoft VSAPI (Virus Scanning API)

Microsoft VSAPI permet à MSME d'analyser les e-mails lorsqu'un utilisateur final y accède à l'aide d'un client de messagerie.

Dans Microsoft Exchange, les e-mails sont stockés dans une base de données appelée banque d'informations Exchange. A la réception d'un nouvel e-mail, Exchange Server informe le client Outlook de la survenue d'une modification. La fonctionnalité d'analyse à l'accès est alors déclenchée.

Cette fonctionnalité est uniquement disponible sur un serveur Microsoft Exchange Server 2007/2010 doté du rôle serveur de boîte aux lettres.

Tableau 5-3 Définition des options

Option	Définition
Activer	Permet d'analyser les e-mails uniquement lorsqu'un utilisateur final y accède à l'aide d'un client de messagerie tel qu'Outlook. Cette fonctionnalité analyse les e-mails déjà disponibles dans la banque d'informations Microsoft Exchange ou en cas de non-concordance dans la référence antivirus.
Analyse proactive	Permet d'analyser les e-mails avant qu'ils ne soient écrits dans la banque d'informations Microsoft Exchange. Activez cette fonctionnalité dans les situations suivantes : • Le logiciel MSME n'est pas configuré sur le serveur de transport HUB et lorsqu'un e-mail infecté atteint le serveur de boîtes aux lettres, il est détecté avant d'être écrit dans la banque d'informations Exchange. • En général, le contenu publié dans une base de données de dossiers publics n'est pas acheminé via un serveur de transport HUB. Afin de garantir l'analyse du contenu avant l'arrivée de l'e-mail dans la banque d'informations, il est conseillé d'activer l'analyse proactive pour les bases de données de dossiers publics.
Analyse de la boîte d'envoi	Permet d'analyser les e-mails contenus dans le dossier Boîte d'envoi. MSME analyse l'e-mail dans la Boîte d'envoi elle-même, avant même qu'il n'atteigne le serveur de transport HUB, réduisant ainsi la charge du serveur HUB.
Limite d'âge inférieure (secondes)	Spécifiez une valeur qui correspond à la période pendant laquelle les e-mails reçus sont analysés. Les e-mails reçus avant ce laps de temps ne seront pas analysés. Par défaut, la valeur est définie sur `86 400` secondes, ce qui équivaut à une journée.
Délai d'expiration de l'analyse (en secondes)	Indique la durée maximale autorisée pour analyser un e-mail. Si l'analyse dépasse la valeur spécifiée, l'action définie sous **Paramètres et diagnostics** | **Paramètres à l'accès** | **Général** | **Sur échec d'analyse** sera exécutée. Par défaut, la valeur est définie sur `180` secondes.
Nombre de threads d'analyse	Indiquez le nombre de threads de pool utilisés pour traiter les éléments dans la file d'attente d'analyse proactive et d'analyse à l'accès. La valeur par défaut est 2 * <nombre de processeurs> + 1. McAfee vous conseille d'activer la case à cocher **Par défaut** pour optimiser les performances.

Paramètres de l'analyse en arrière-plan

Vous avez la possibilité d'analyser méthodiquement les messages souhaités stockés dans une base de données. Pour chaque base de données, un thread exécuté en dessous du niveau de priorité normal énumère toutes les données incluses dans la base de données, puis demande à MSME d'analyser le contenu comme il convient.

Tableau 5-4 Définition des options

Option	Définition
Activer	Permet d'analyser la totalité de la base de données en arrière-plan, après une attaque virale. Par défaut, cette option est désactivée.
Planifier	Permet de planifier les heures auxquelles l'analyse en arrière-plan doit être activée ou désactivée. • Cliquez sur **Activer à** pour indiquer l'heure à laquelle l'analyse en arrière-plan doit débuter. • Cliquez sur **Désactiver à** pour indiquer l'heure à laquelle l'analyse en arrière-plan doit s'arrêter.  • Planifiez l'exécution de cette tâche pendant les heures creuses en semaine ou le week-end. • Si vous n'avez pas défini de planification, l'analyse en arrière-plan débute dès qu'une mise à jour des fichiers DAT se produit.
Uniquement les messages avec une pièce jointe	Permet d'analyser uniquement les e-mails dotés de pièces jointes. Cette fonctionnalité s'avère pratique lorsqu'un virus précis se propageant via les pièces jointes vous inquiète. Etant donné que les e-mails dotés de pièces jointes sont plus vulnérables, s'ils incluent du contenu malveillant, tous les virus ou fichiers exécutables seront remplacés au cours de cette tâche. L'activation de cette fonctionnalité permet de gagner du temps, car MSME analyse uniquement les e-mails dotés de pièces jointes.
Uniquement les éléments non analysés	Permet d'analyser des e-mails jamais analysés. Activez cette option dans les scénarios où vous souhaitez analyser des éléments non analysés suite à la désactivation de Microsoft VSAPI sur le serveur de boîtes aux lettres pendant un certain temps.
Forcer l'analyse complète	Permet d'analyser des éléments, qu'ils disposent ou non d'une référence d'analyse antivirus (AV).
Mettre à jour la référence d'analyse	Permet de mettre à jour les e-mails avec la référence antivirus la plus récente.
Date de début	Permet d'effectuer une analyse en arrière-plan uniquement sur les e-mails reçus à compter de la date indiquée.
Date de fin	Permet d'effectuer une analyse en arrière-plan uniquement sur les e-mails reçus jusqu'à la date indiquée. Sélectionnez **Jusqu'à cette date** pour analyser les e-mails jusqu'à la date système actuelle.

Paramètres d'analyse du trafic

L'analyse du trafic vous permet d'analyser le trafic SMTP avant qu'il n'entre dans la banque d'informations Exchange. La fonctionnalité d'analyse du trafic SMTP peut s'appliquer aux e-mails acheminés, c'est-à-dire non destinés au serveur local, et en arrêter la remise.

Tableau 5-5 Définition des options

Option	Définition
Activer	Permet d'activer l'analyse au niveau du service Exchange Transport. Par défaut, cette option est activée. Cette option fonctionne uniquement sur les serveurs Microsoft Exchange disposant des rôles serveur de transport Edge, serveur de transport Hub ou serveur de boîte aux lettres + serveur de transport Hub.
Référence d'analyse du trafic	Sélectionnez cette option pour appliquer des signatures DAT à l'en-tête d'e-mail, afin que les e-mails soient analysés une seule fois au niveau du rôle Boîte aux lettres. **Paramètres recommandés :** si vous avez activé l'analyse du trafic, veillez à activer également cette option.
Ne pas analyser les e-mails dont la taille est supérieure à	Excluez les e-mails de l'analyse à l'accès d'après leur taille. Vous pouvez définir la taille de fichier en Ko ou en Mo. Il est conseillé d'analyser tous les fichiers avant d'y accéder, afin de protéger vos systèmes contre toute menace potentielle.
Analyse en fonction de la direction	Configurez les paramètres d'analyse à l'accès en fonction du flux d'e-mails.
Analyser les messages entrants	Permet d'analyser les e-mails qui entrent dans le serveur Exchange ou l'organisation Exchange.
Analyser les messages sortants	Permet d'analyser les e-mails qui quittent votre serveur Exchange ou votre organisation Exchange. Les e-mails sont désignés comme étant sortants si au moins un destinataire dispose d'une adresse externe.
Analyser les messages internes	Permet d'analyser les e-mails qui sont acheminés d'un emplacement de votre domaine vers un autre emplacement du même domaine. Tout élément inclus dans le domaine faisant autorité de votre serveur Exchange est considéré comme domaine interne. Les e-mails sont désignés comme internes s'ils ont été émis depuis un domaine donné et que tous ses destinataires se trouvent dans le même domaine.

Paramètres à la demande

Accédez à la page **Paramètres à la demande** pour modifier les informations d'identification de mot de passe de **MSMEODUser**.

McAfee Security for Microsoft Exchange crée un utilisateur nommé **MSMEODuser** dans l'annuaire Active Directory pendant l'installation du produit sur le serveur de boîte aux lettres. L'exécution d'analyses à la demande des boîtes aux lettres requiert la présence de cet utilisateur.

Par souci de conformité à la stratégie de sécurité de votre organisation, vous devez peut-être mettre à jour le mot de passe de **MSMEODUser** à intervalles réguliers.

A partir de l'interface, accédez à **Paramètres et diagnostics** | **Paramètres à la demande**.

Option	Définition
Nom d'utilisateur	**MSMEODUser** — L'utilisateur qui effectue l'analyse à la demande. Il s'agit d'un champ en lecture seule.
Saisir le mot de passe	Saisissez le mot de passe.
Confirmer le mot de passe	Confirmez le mot de passe.
Réinitialiser également ce mot de passe dans LDAP	Sélectionnez cette option pour synchroniser la mise à jour du mot de passe avec l'Active Directory et les autres Exchange Servers. Vérifiez cette option uniquement lorsque vous lancez la réinitialisation du mot de passe à partir de la page **Paramètres à la demande**.

Vous pouvez mettre à jour le mot de passe **MSMEODUser** de deux manières différentes :

- Réinitialisez le mot de passe dans l'annuaire Active Directory, puis mettez à jour le mot de passe sur la page **Paramètres à la demande**.
- Réinitialisez le mot de passe à partir de la page **Paramètres à la demande**.

Réinitialiser le mot de passe à l'aide d'Active Directory	Réinitialiser le mot de passe à l'aide de la page Paramètres à la demande
1 Mettez à jour le mot de passe dans l'annuaire Active Directory. 2 Accédez à n'importe quel système de rôle de boîte aux lettres au sein du même annuaire Active Directory. 3 Lancez l'interface de McAfee Security for Microsoft Exchange. 4 A partir de **Paramètres et diagnostics**, accédez à la page **Paramètres à la demande**, puis mettez à jour le mot de passe. 5 Désélectionnez l'option **Réinitialiser le mot de passe dans LDAP également**. 6 Cliquez sur **Appliquer**.	1 Lancez l'interface de McAfee Security for Microsoft Exchange. 2 A partir de **Paramètres et diagnostics**, accédez à la page **Paramètres à la demande**, puis mettez à jour le mot de passe. 3 Vérifiez l'option **Réinitialiser le mot de passe dans LDAP également** pour vous assurer que la mise à jour du mot de passe est synchronisée avec l'annuaire Active Directory. 4 Cliquez sur **Appliquer**.

Pour les systèmes managés, vous pouvez mettre à jour le mot de passe **MSMEODUser** à partir de ePolicy Orchestrator.

L'application de ces paramètres à tous les serveurs Exchange dans le domaine peut prendre jusqu'à une minute. Exécutez une analyse à la demande après la mise à jour du mot de passe à des fins de vérification.

Pour plus d'informations sur l'utilisateur **MSMEODUser**, consultez l'article KB82332 dans McAfee KnowledgeBase.

Configuration des paramètres d'exclusion de boîtes aux lettres

Configurez les boîtes aux lettres ou dossiers qui doivent être exclu(e)s d'une analyse VSAPI.

Configurez les paramètres d'exclusion de boîtes aux lettres dans des cas de figure précis :

- Les dirigeants de l'entreprise ne souhaitent pas que leurs e-mails soient analysés.
- La politique d'entreprise identifie les dossiers à ne pas analyser.
- Les dossiers qui doivent être exclus de l'analyse.

McAfee déconseille d'exclure des boîtes aux lettres de l'analyse et rejette toute responsabilité en cas de boîtes aux lettres infectées en raison de paramètres d'exclusion.

Procédure

1 Cliquez sur **Paramètres et diagnostics** | **Paramètres d'exclusion de la boîte aux lettres**. La page **Paramètres d'exclusion de la boîte aux lettres** s'affiche.

2 Pour exclure la boîte aux lettres ou le sous-dossier :

Pour exclure une boîte aux lettres	Pour exclure un dossier dans la boîte aux lettres
1 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez une boîte aux lettres, puis cliquez sur >>. La boîte aux lettres sélectionnée est déplacée vers le volet **Boîtes aux lettres à exclure**. Répétez cette étape pour toutes les boîtes aux lettres à exclure d'une analyse VSAPI. Pour retirer une boîte aux lettres de la liste d'exclusion, sélectionnez-la dans le volet **Boîtes aux lettres à exclure**, puis cliquez sur << pour la déplacer vers la liste **Boîtes aux lettres disponibles**. Lorsqu'une boîte aux lettres est ajoutée au volet **Boîtes aux lettres à exclure**, tous les dossiers dans la boîte aux lettres sont exclus de l'analyse.	1 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez une boîte aux lettres. 2 Dans la zone **Dossiers dans la boîte aux lettres à exclure**, saisissez le nom de nom de dossier à exclure, puis cliquez sur >>. Le dossier de boîte aux lettres sélectionnée est déplacé vers le volet **Boîtes aux lettres à exclure**. Vous pouvez utiliser un caractère générique pour exclure plusieurs dossiers de l'analyse VSAPI. Pour plus d'informations, voir Utilisation du caractère générique pour exclure les dossiers de boîte aux lettres.

Si vous configurez des exclusions de boîte aux lettres à partir de ePolicy Orchestrator, vous devez fournir le chemin complet manuellement.

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

Cette exclusion ignore **Analyse de la boîte d'envoi** dans les paramètres **Microsoft Virus Scanning API (VSAPI)** sur la page **Paramètres à l'accès** que vous avez déjà configurée. Par exemple, si vous excluez l'analyse de la boîte d'envoi pour un utilisateur, le paramètre d'exclusion de boîtes aux lettres ignore l'analyse de boîte d'envoi globale.

Pour plus d'informations sur les exemples d'exclusion de boîtes aux lettres, voir *Exemples d'utilisation de caractères génériques pour les exclusions de boîtes aux lettres*.

Exemples d'utilisation de caractères génériques pour les exclusions de boîtes aux lettres

Vous pouvez utiliser une virgule comme séparateur ou le caractère générique * pour exclure les dossiers de l'analyse VSAPI au niveau de la boîte aux lettres et au niveau de la base de données.

Tableau 5-6 Exemples

Niveau...	A exclure...	Configurer...
Au niveau de la base de données	Les dossiers **Brouillon** de toutes les boîtes aux lettres dans la base de données.	1 A partir de l'interface du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres d'exclusion de la boîte aux lettres**. 2 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez la base de données. 3 Dans la boîte **Dossiers dans la boîte aux lettres à exclure**, saisissez **Brouillon**, cliquez sur >>, puis cliquez sur **Appliquer**. Le dossier de boîte aux lettres sélectionnée est répertorié dans le volet **Boîtes aux lettres à exclure**. Vous ne pouvez pas sélectionner une base de données à exclure sans spécifier de dossiers à exclure.
	Tous les dossiers dans toutes les boîtes aux lettres qui commencent avec le nom **personne** dans la base de données.	1 A partir de l'interface du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres d'exclusion de la boîte aux lettres**. 2 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez la base de données. 3 Dans la boîte **Dossiers dans la boîte aux lettres à exclure**, saisissez **personne***, cliquez sur >>, puis cliquez sur **Appliquer**. Le dossier de boîte aux lettres sélectionnée est répertorié dans le volet **Boîtes aux lettres à exclure**.
Au niveau de la boîte aux lettres	Plusieurs dossiers dans une boîte aux lettres à l'aide d'une virgule comme séparateur. Par exemple, vous pouvez exclure les dossiers Données1, Projet1, et Rapport1 situés dans la **Boîte de réception**.	1 A partir de l'interface du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres d'exclusion de la boîte aux lettres**. 2 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez une boîte aux lettres. 3 Dans la boîte **Dossiers dans la boîte aux lettres à exclure**, saisissez `Boîte aux lettres\Données1,Boîte aux lettres\Projet1,Boîte aux lettres\Rapport1`, cliquez sur >>, puis cliquez sur **Appliquer**.
	Dossiers et leurs sous-dossiers. • Vous pouvez exclure les e-mails dans les sous-dossiers mais analyser les e-mails dans un dossier. • Vous pouvez exclure les e-mails et les sous-dossiers d'un dossier.	1 A partir de l'interface du produit, cliquez sur **Paramètres et diagnostics** | **Paramètres d'exclusion de la boîte aux lettres**. 2 A partir du volet **Boîtes aux lettres disponibles**, sélectionnez une boîte aux lettres. • `Boîte aux lettres\Personnel*` — Pour exclure les e-mails et les sous-dossiers dans le dossier **Personnel** de l'analyse VSAPI. • `Boîte aux lettres\Personnel*` — Pour exclure tous les sous-dossiers dans le dossier **Personnel** de l'analyse VSAPI. Les e-mails dans le dossier **Personnel** ne sont pas exclus de l'analyse VSAPI.

Paramètres de notification

Les paramètres de notification permettent de configurer le contenu et l'adresse SMTP nécessaires à l'administrateur pour envoyer des notifications par e-mail suite à la mise en quarantaine d'un e-mail.

A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Notifications** pour configurer les paramètres de notification.

A la page **Notifications**, vous pouvez utiliser les options suivantes :

- **Paramètres** : permet de définir un compte de messagerie pour la réception de notifications relatives à la mise en quarantaine d'e-mails. De plus, lorsqu'un e-mail est mis en quarantaine en raison d'un analyseur ou d'un filtre précis, vous avez la possibilité d'envoyer des e-mails de notification à des réviseurs spécifiques ou à des listes de distribution.

  Assurez-vous que les adresses e-mail sont mises à jour comme requis pour les systèmes ou les systèmes de groupe sur la page **Notification** pour recevoir les notifications pour systèmes managés et autonomes.

  Pour envoyer des notifications par e-mail à une liste de distribution, spécifiez l'adresse SMTP de cette dernière.

- **Modèle** : permet de créer un e-mail de notification personnalisé qui est envoyé à des utilisateurs précis suite à la mise en quarantaine d'un e-mail.

- **Alertes sur l'intégrité du produit** : permet de définir des alertes relatives à l'intégrité des produits qui sont envoyées par e-mail à l'administrateur une fois par jour ou dès qu'un événement donné se produit (par ex. problème avec la base de données Postgres ou échec du chargement d'un service).

  Lors de la configuration du produit, comme la notification ou le nom de stratégie, assurez-vous de ne pas utiliser de caractères qui peuvent provoquer une vulnérabilité Cross Site Scripting (XSS). Pour la liste de caractères à éviter, consultez l'article KB82214 de McAfee KnowledgeBase.

Configuration des paramètres de notification

Configurez un compte de messagerie pour la réception de notifications relatives à la mise en quarantaine d'e-mails. Envoyez également des e-mails de notification à des réviseurs précis ou à des listes de distribution suite à la détection d'un e-mail.

Procédure

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

2 Dans l'onglet **Notifications** | **Paramètres**, vous pouvez utiliser les options suivantes :

Tableau 5-7 Définition des options

Option	Définition
Général	Permet de définir des paramètres de notification par e-mail simples.
E-mail de l'administrateur	Permet de notifier l'administrateur Microsoft Exchange en cas de survenue d'un événement de type alerte ou action de mise en quarantaine. • Pour envoyer des notifications par e-mail à plusieurs utilisateurs, utilisez un point-virgule (;) comme séparateur. • Pour envoyer des notifications par e-mail à une liste de distribution, spécifiez l'adresse SMTP de cette dernière.

Tableau 5-7 Définition des options *(suite)*

Option	Définition
E-mail de l'expéditeur	Permet de spécifier l'e-mail de l'expéditeur dans le champ **De** de l'e-mail de notification. McAfee recommande de ne pas modifier l'adresse **E-mail de l'expéditeur**, car le logiciel crée et utilise cette adresse pour plusieurs processus. Si vous modifiez cette adresse e-mail et que vous n'activez pas le connecteur de réception **Anonyme** dans Microsoft Exchange, vous ne recevrez pas les notifications du produit.
Activer la notification concernant les résultats de la tâche	Permet d'envoyer des e-mails avec l'analyse à la demande et les résultats des tâches de mise à jour. L'e-mail est au format HTML et possède les mêmes données et format que la fenêtre **Résultat de tâches** dans l'interface utilisateur. Il est possible d'activer et de désactiver cette fonctionnalité au moyen de cette option. Par défaut, cette fonctionnalité est désactivée.
Options avancées	Permet de définir des paramètres de notification avancés tels que la spécification d'adresses e-mail et la ligne de l'objet de chaque analyseur ou filtre.
Corps de l'e-mail	Permet de définir un corps d'e-mail générique pour toutes les notifications.

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

MSME fournit une sécurité améliorée en ne prenant pas en charge les balises HTML présentant une vulnérabilité XSS. McAfee recommande de supprimer les balises HTML présentant une vulnérabilité XSS du modèle de notification existant avant la mise à niveau. Dans le cas contraire, après la mise à niveau, si vous tentez de modifier les modèles de notification contenant des balises non prises en charge, vous serez invité à supprimer les balises non prises en charge du modèle ou à utiliser le modèle sans modification. Pour la liste des balises HTML prises en charge, consultez l'article KB82214 de McAfee KnowledgeBase.

Modification du modèle de notification

Affichez ou modifiez le corps du message de l'e-mail de notification envoyé à l'utilisateur final.

Procédure

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

2 Sous l'onglet **Notifications** | **Modèle**, vous pouvez utiliser les options suivantes :

Tableau 5-8 Définition des options

Option	Définition
Modèle	Permet d'afficher le modèle de notification d'un utilisateur donné. Les options disponibles sont les suivantes : • **Expéditeur interne** • **Destinataire interne** • **Expéditeur externe** • **Destinataire externe** Vous pouvez définir le texte de la notification en fonction de chacun de ces types d'utilisateur.
Objet	Permet de spécifier la ligne d'objet de l'e-mail de notification. Par défaut, l'objet de la notification correspond à **Alerte McAfee Security for Microsoft Exchange**.

Tableau 5-8 Définition des options *(suite)*

Option	Définition
Texte de la notification	Permet d'afficher un aperçu du corps de l'e-mail de notification, en fonction du **Modèle** sélectionné. Le texte de la notification contient des informations relatives à l'élément mis en quarantaine, notamment la date et l'heure, l'objet, l'action entreprise, etc.
Modifier	Permet de modifier le texte de la notification en langage HTML, au format texte simple. Une fois la notification modifiée pour répondre aux exigences de l'entreprise, cliquez sur **Enregistrer** pour appliquer les modifications.

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

Vous venez d'afficher ou de modifier le modèle de notification. Pour plus d'informations sur les champs de notification disponibles, consultez la section *Champs de notification disponibles*.

Champs de notification disponibles

Vous avez la possibilité d'inclure les champs suivants dans vos notifications. Par exemple, si vous souhaitez inclure le nom de l'élément détecté et l'action entreprise correspondante, utilisez **%vrs%** et **%act%** à la page **Paramètres et diagnostics | Notifications | Modèle**.

Tableau 5-9 Champs de notification disponibles

Options de champs de notification	Description
%dts%	Date et heure
%sdr%	Expéditeur
%ftr%	Filtre
%fln%	Nom du fichier
%rul%	Nom de la règle
%act%	Action entreprise
%fdr%	Dossier
%vrs%	Nom de la détection
%trs%	Etat (état du train)
%tik%	Numéro de ticket
%idy%	Analysé par
%psn%	Nom de la stratégie
%svr%	Serveur
%avd%	Fichier DAT de l'antivirus
%ave%	Moteur antivirus
%rpt%	Destinataire
%rsn%	Raison
%sbj%	Objet
%ssc%	Score de spam
%ase%	Moteur antispam
%asr%	Règles antispam

Activation des alertes sur l'état de fonctionnement des produits

Envoyez à l'administrateur Microsoft Exchange des notifications immédiates ou quotidiennes pour l'informer de l'échec d'une tâche relative à un produit.

Procédure

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

2 Sous l'onglet **Notifications** | **Alertes sur la santé du produit**, vous pouvez utiliser les options suivantes :

Tableau 5-10 Définition des options

Option	Définition
Activer	Permet d'activer l'envoi de notifications d'alertes sur l'état de fonctionnement des produits à l'administrateur suite à l'échec d'une tâche relative à un produit.
Alerter ePolicy Orchestrator	Permet d'alerter le serveur McAfee ePolicy Orchestrator qui manage ce serveur MSME en cas d'échec d'une tâche relative à un produit.
Alerter l'administrateur	Permet d'envoyer des alertes relatives à l'état de fonctionnement des produits à l'adresse e-mail spécifiée sous **Paramètres et diagnostics** | **Notifications** | **Paramètres** | **E-mail de l'administrateur**.
Avertir lorsque	Permet de prévenir l'administrateur en cas d'échec de l'une des tâches produit sélectionnées. Les options suivantes sont disponibles pour l'envoi à l'administrateur d'alertes relatives à l'état de fonctionnement des produits : Ces options varient selon le rôle de votre serveur Exchange. • **Le téléchargement des fichiers DAT/du moteur antivirus échoue** • **Le téléchargement des règles anti-spam échoue** • **Le téléchargement du moteur antivirus échoue** • **Le chargement du module TransportScan échoue** • **Le chargement du module VSAPI échoue** • **Le processus RPCServ se ferme de manière inattendue** • **Le processus DLLHost se ferme de manière inattendue** • **Le processus Postgres échoue** • **Echec de mise en quarantaine ou de journalisation des détections par Postgres** • **Echec de l'initialisation de la base de données par Postgres** • **Echec de l'enregistrement par Postgres** • **Echec de l'analyse à la demande** • **Espace disque de la base de données en dessous du seuil** • **Echec de démarrage du service du produit** • **L'analyse de la réputation des fichiers de McAfee Global Threat Intelligence échoue**
Immédiate	Envoie une notification à l'administrateur immédiatement après l'échec de la tâche.
Quotidienne	En cas d'échec d'une tâche, envoie une notification à l'administrateur une fois par jour, à une heure précise.

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

Vous avez à présent terminé l'activation de la fonctionnalité **Alertes sur la santé du produit**.

Paramètres antispam

Définissez les paramètres du dossier de courrier indésirable vers lequel le spam détecté sur un serveur de transport Edge ou Hub doit être transféré. Activez ou désactivez également les paramètres relatifs aux fonctionnalités de réputation des messages McAfee GTI et de réputation des adresses IP McAfee GTI.

Tableau 5-11 Définition des options

Option	Définition
Adresse du dossier Courrier indésirable du système	Spécifiez l'adresse e-mail à laquelle tous les e-mails classés comme spam doivent être envoyés.
Réputation des messages McAfee GTI	La réputation des messages McAfee Global Threat Intelligence est le service de réputation de message et d'expéditeur exhaustif, en temps réel, basé sur le cloud de McAfee qui permet à MSME de protéger votre serveur Exchange contre les menaces à la fois connues et émergentes basées sur les messages (telles que le spam). MSME reçoit tous les jours des millions de requêtes d'e-mail, prend une empreinte du contenu des messages (par rapport au contenu lui-même, pour des raisons de confidentialité) et analyse ces données en fonction de nombreux paramètres. La réputation des messages est combinée à différents facteurs tels que les modèles d'envoi de spam et le comportement des adresses IP pour déterminer si le message en question peut être malveillant. Le score est non seulement calculé en fonction de l'intelligence collective des capteurs interrogeant le cloud McAfee et de l'analyse réalisée par les chercheurs de McAfee Labs Labs et des outils automatisés, mais aussi de la corrélation d'informations d'intelligence intervectorielles issues de données de menaces de fichiers, du web et de réseau. MSME utilise ce score pour identifier une action en fonction de la stratégie locale **Gestionnaire de stratégies** | **Passerelle**.
Activer	Permet de bloquer les e-mails au niveau de la passerelle en fonction de leur score de réputation.
Effectuer une réputation des messages après l'antispam	Permet d'effectuer une action de réputation des messages McAfee GTI après une analyse en fonction de la stratégie MSME.
Seuil de réputation des messages	Spécifiez une valeur de seuil destinée à bloquer les e-mails en fonction du score de réputation des messages. Par défaut, la valeur est définie sur `80`.
Action à entreprendre	Sélectionnez les options suivantes en fonction de vos besoins : • **Déplacer et mettre en quarantaine** : permet de supprimer l'e-mail et de le mettre en quarantaine dans la base de données. Lorsqu'un e-mail est supprimé en raison de ce paramètre, l'expéditeur n'en est pas informé lors du statut de remise du courrier électronique. • **Score de réussite pour le moteur antispam** : permet d'envoyer au moteur antispam le score de réputation des messages détecté par le service McAfee GTI. Cette option est disponible uniquement si vous avez activé l'option **Effectuer une réputation des messages après l'antispam**.
Réputation des adresses IP McAfee GTI	La fonctionnalité de réputation des adresses IP agit comme le premier niveau de protection de votre environnement Exchange, en protégeant votre serveur Exchange contre les sources d'e-mail suspectes. Cette fonctionnalité vous permet de tirer parti des informations sur les menaces recueillies par le service McAfee Global Threat Intelligence afin d'éviter les dommages et le vol de données en bloquant les e-mails au niveau de la passerelle, en fonction de l'adresse IP source.
Activer	Permet de bloquer les e-mails au niveau de la passerelle en fonction de l'adresse IP source.

Tableau 5-11 Définition des options *(suite)*

Option	Définition
Seuil de réputation des adresses IP	Spécifiez une valeur de seuil destinée à bloquer les e-mails en fonction du score de réputation des adresses IP. L'action est appliquée à toutes les adresses IP dont le score de réputation est supérieur au seuil sélectionné. L'acheminement de tous les autres e-mails est autorisé. Vous pouvez mettre sur liste blanche les adresses IP légitimes qui sont bloquées par les paramètres **Seuil de réputation IP** sur la page **Paramètres antispam** par la modification des valeurs de Registre. Après l'inclusion dans la liste blanche de l'adresse IP, les e-mails provenant de l'adresse IP incluse dans liste blanche sont autorisés, indépendamment de leurs scores de réputation. **Important** : la mise sur liste blanche d'adresses IP ignore uniquement les paramètres de **Seuil de réputation des adresses IP**. MSME poursuit l'analyse de l'e-mail pour identifier du contenu corrompu ou chiffré, le filtre de fichiers, l'analyse de contenu, la réputation d'URL et contre les logiciels malveillants. En cas de détection positive, une action est entreprise en fonction de la configuration du produit. Avant la mise sur liste blanche de l'adresse IP, McAfee recommande de vérifier le score de réputation de l'adresse IP à partir de www.trustedsource.org pour vérifier sa légitimité. McAfee rejette toute responsabilité en cas de boîtes aux lettres infectées par une adresse IP incluse dans la liste blanche. Pour plus d'informations sur la configuration des listes blanches d'adresses IP pour l'Agent IP à l'aide du registre, consultez l'article KB82216 de la base de connaissances McAfee.
Action à entreprendre	Sélectionnez l'une ou l'autre option pour définir l'action à entreprendre concernant un e-mail, en fonction du score de réputation de l'adresse IP source : • **Abandonner la connexion et consigner** : permet de supprimer l'e-mail provenant de l'adresse IP source et de consigner l'action entreprise concernant l'élément. • **Rejeter la connexion et consigner** : permet de rejeter l'e-mail provenant de l'adresse IP source (en notifiant l'expéditeur) et de consigner l'action entreprise concernant l'élément.
Filtre SPF	Protège vos systèmes contre les e-mails d'usurpation et permet de configurer l'exécution d'actions en cas de réception de messages d'erreur matérielle ou logicielle.

Paramètres des éléments détectés

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

Configurez et gérez les référentiels de quarantaine à l'aide des composants suivants :

- **McAfee Quarantine Manager** : permet de mettre en quarantaine les éléments détectés sur le serveur MQM.
- **Base de données locale** : permet de mettre en quarantaine les éléments détectés sur le serveur MSME local.

Mise en quarantaine à l'aide de McAfee Quarantine Manager

Spécifiez les paramètres de référentiel pour la mise en quarantaine des éléments détectés par MSME sur un serveur McAfee Quarantine Manager.

Les produits McAfee tels que McAfee Security for Microsoft Exchange et McAfee Email Gateway utilisent un numéro de port préaffecté pour envoyer les informations de détection à McAfee Quarantine Manager. McAfee Quarantine Manager utilise également le même numéro de port par défaut pour publier ou envoyer des informations de configuration concernant les e-mails détectés au produit McAfee.

Le port de communication mentionné dans l'interface utilisateur de McAfee Security for Microsoft Exchange et McAfee Quarantine Manager doit être le même.

Vous pouvez utiliser McAfee Quarantine Manager pour consolider la fonctionnalité de gestion antispam et de mise en quarantaine. Il constitue un point central à partir duquel vous pouvez analyser et traiter de façon adéquate les e-mails et les fichiers mis en quarantaine.

Ce guide ne fournit pas d'informations détaillées sur l'installation et l'utilisation du logiciel McAfee Quarantine Manager. Plus d'informations, consultez la documentation produit de McAfee Quarantine Manager.

Procédure

1. Installez le logiciel McAfee Security for Microsoft Exchange sur <server 1>.
2. Installez le logiciel McAfee Quarantine Manager pris en charge sur <server 2>.
3. Lancez l'interface utilisateur MSME à partir de <server 1>.
4. A partir de l'interface utilisateur du produit, cliquez sur **Paramètres et diagnostics** | **Eléments détectés**.

   La page **Eléments détectés** s'affiche.
5. Dans la section **McAfee Quarantine Manager**, sélectionnez **Activer**.
6. Dans **Mode de communication**, sélectionnez le mode.
   - **RPC** — RPC (Remote Procedure Call) est un mécanisme de communication qui requiert une connexion ininterrompue pour communiquer avec le serveur McAfee Quarantine Manager. En cas d'échec de la communication avec le serveur McAfee Quarantine Manager, les processus comme la mise en quarantaine et la libération sont interrompus.
   - **HTTP** — Un mécanisme de communication sans état pour communiquer avec le serveur McAfee Quarantine Manager. En cas d'échec de communication avec le serveur McAfee Quarantine Manager, les éléments sont stockés dans la base de données locale jusqu'à la restauration de la connexion. MSME tente d'envoyer les éléments mis en quarantaine à MQM à trois reprises. Si les trois tentatives échouent, l'entrée de journal du produit est créée et l'élément est stocké dans la base de données locale.
   - **HTTPs** — Un mécanisme de communication HTTP sécurisé dans lequel les données sont transférées au format chiffré.

     McAfee recommande d'utiliser le canal de communication HTTP/HTTPs, car les connexions sans état assurent que le logiciel peut communiquer sans problème avec McAfee Quarantine Manager.
7. Dans le champ **Adresse IP**, indiquez l'adresse IP du serveur MQM.

8 Dans **Port** et **Port de rappel**, indiquez les valeurs par défaut.

Mode de communication	Valeur du port	Port de rappel	Intervalle de mise à jour de la liste noire et la liste blanche (heures)
RPC	49500	49500	–
HTTP	80	–	4
HTTPs	443	–	4

Modifiez cette valeur uniquement si vous avez configuré une valeur de port différente sur le serveur McAfee Quarantine Manager.

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

Vous avez correctement configuré le serveur MSME pour l'application de la mise en quarantaine des éléments détectés sur le serveur MQM.

Mise en quarantaine à l'aide de la base de données locale

Spécifiez les paramètres de référentiel pour la mise en quarantaine des éléments détectés par MSME dans une base de données PostgreSQL située sur le serveur MSME local.

Procédure

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

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

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

Tableau 5-12 Définition des options

Option	Définition
Spécifier l'emplacement de la base de données	Permet d'activer l'option **Emplacement de la base de données** afin de stocker les éléments mis en quarantaine détectés par MSME.
Emplacement de la base de données	Permet de spécifier le chemin d'accès à l'emplacement de la base de données dans laquelle les éléments détectés par MSME peuvent être stockés. Vous pouvez sélectionner : • **<Dossier d'installation>** : permet de créer les sous-dossiers de la base de données sous le répertoire d'installation de MSME. • **<Lecteur système>** : permet de créer les sous-dossiers de la base de données sous le répertoire `C:\Windows\system32`. • **<Fichiers programme>** : permet de créer les sous-dossiers de la base de données sous le répertoire `C:\Program Files (x86)` de Windows. • **<Dossier Windows>** : permet de créer les sous-dossiers de la base de données sous le répertoire `C:\Windows`. • **<Dossier de données>** : permet de créer les sous-dossiers de la base de données sous le répertoire `C:\ProgramData\`. • **<Chemin d'accès complet>** : permet de stocker la base de données MSME dans le chemin d'accès complet indiqué. Spécifiez le chemin d'accès au sous-dossier dans le champ situé en regard de la liste déroulante. Par défaut, il s'agit du chemin d'accès suivant : `McAfee\MSME\Data\`

Tableau 5-12 Définition des options *(suite)*

Option	Définition
Taille maximale de l'élément (Mo)	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 999, la valeur par défaut étant 100.
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 **Eléments 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 30.
Intervalle de vérification de la taille du disque (Minute)	Permet de spécifier la fréquence à laquelle MSME doit vérifier l'espace disque disponible. Vous pouvez indiquer une valeur comprise entre 6 et 2 880, la valeur par défaut étant 6.
Seuil d'espace disque (Mo)	Permet de spécifier le seuil auquel un avertissement est envoyé à l'administrateur concernant l'espace disque faible. Vous pouvez indiquer une valeur comprise entre 1 et 512 000, la valeur par défaut étant 2 048. Assurez-vous que l'option **Espace disque de la base de données en dessous du seuil** est activée sous **Paramètres et diagnostics** | **Notifications** | **Alertes sur la santé du produit** | **Avertir lorsque**.
Fréquence de purge des éléments anciens	Permet de spécifier la fréquence à laquelle les anciens éléments marqués pour la suppression sont supprimés de la base de données MSME. La valeur par défaut est **Chaque mois**.
Fréquence d'optimisation	Permet de récupérer l'espace disque occupé par les enregistrements de base de données supprimés. Selon la valeur attribuée à l'option **Age maximal de l'élément (jours)**, les anciens enregistrements seront supprimés si vous avez planifié une tâche de purge. Une fois les anciens enregistrements supprimés, MSME utilisera encore l'espace disque spécifié dans le champ **Seuil d'espace disque (Mo)**, même si la base de données de quarantaine n'a pas atteint la limite de taille. Afin d'optimiser et de réduire la base de données, planifiez une tâche d'optimisation. La valeur par défaut est **Chaque mois**. Pensez à toujours planifier une tâche d'optimisation quelques heures après avoir effectué une tâche de purge.
Modifier la planification	Permet de modifier la planification de la tâche de purge ou d'optimisation. Cliquez sur **Enregistrer** après avoir modifié la planification.

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

Vous avez à présent terminé la configuration du serveur MSME pour qu'il mette en quarantaine les 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 **Eléments récemment analysés**, ainsi que l'intervalle de rapport de statut.

Procédure

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 5-13 Définition des options

Option	Définition
Actualisation automatique	Permet de spécifier si les informations visibles sur le compteur **Tableau de bord**	**Statistiques** doivent s'actualiser automatiquement.
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 à la section **Tableau de bord**	**Rapports**	**Eléments récemment analysés**. Vous pouvez indiquer une valeur comprise entre 10 et 100, la valeur par défaut étant 10.
Echelle du graphique (unités)	Permet de spécifier les unités de mesure de l'échelle du graphique à barres généré à 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), comme les rapports de statut et les rapports de configuration. 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 disponibles à la section **Tableau de bord** | **Graphique** en vue d'améliorer les paramètres des graphiques et diagrammes.

Procédure

1 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 5-14 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, les moyens de réduire les problèmes et les solutions adaptées aux problèmes rencontrés lors de l'utilisation de MSME.

Dans la page **Paramètres et diagnostics** | **Diagnostics**, vous pouvez utiliser 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.
- **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 journal du produit de MSME (`productlog.bin`). Les modifications apportées à ce paramètre sont ensuite répercutées sur la page **Paramètres et diagnostics** | **Journal du produit**.
- **Service de rapport d'erreurs** : permet de configurer les paramètres de détection des exceptions (telles que les blocages système) et de notification à l'utilisateur via un rapport.

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 **Aucun** au paramètre **Niveau**. 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

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

La page **Diagnostics** s'affiche.

2 Sous l'onglet **Journalisation de débogage**, vous pouvez utiliser les options suivantes :

Tableau 5-15 Définition des options

Option	Définition
Niveau	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 : • **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	Permet de spécifier la taille maximale des fichiers journaux de débogage. Vous pouvez indiquer une valeur comprise entre 1 Ko et 2 000 Mo. 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.

Tableau 5-15 Définition des options *(suite)*

Option	Définition
Activer la journalisation de débogage	Permet de modifier l'emplacement par défaut de journalisation des fichiers de débogage. Lorsque cette option est désactivée, les fichiers journaux de débogage sont stockés sous le répertoire par défaut `<Install Folder>\bin\debuglogs`.
Emplacement du fichier	Permet de spécifier le chemin d'accès à l'emplacement du fichier journal de débogage dans lequel les événements déclenchés par MSME peuvent être stockés. Vous pouvez sélectionner : • **<Dossier d'installation>** : permet de créer les fichiers journaux de débogage sous le répertoire d'installation de MSME. • **<Lecteur système>** : permet de créer les fichiers journaux de débogage sous le répertoire `C:\Windows\system32`. • **<Fichiers programme>** : permet de créer les fichiers journaux de débogage sous le répertoire `C:\Program Files (x86)` de Windows. • **<Dossier Windows>** : permet de créer les fichiers journaux de débogage sous le répertoire `C:\Windows`. • **<Dossier de données>** : permet de créer les fichiers journaux de débogage sous le répertoire `C:\ProgramData\`. • **<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. 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.

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.

Pour plus d'informations sur la génération de journaux de conteneur Exchange Web Services (EWS) pour la tâche d'analyse à la demande, consultez l'article KB82215 dans McAfee KnowledgeBase.

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 journalisation des événements

Configurez les paramètres de journalisation des types d'événements MSME dans le **Journal du produit** et dans l'Observateur d'événements Windows.

Un événement désigne une action que vous pouvez effectuer et qui est surveillée par MSME. 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 permet aux administrateurs système d'obtenir plus facilement des informations sur les problèmes qui se produisent.

Procédure

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 5-16 Définition des options

Option	Définition
Journal du produit	Permet de consigner les événements MSME 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 les événements MSME dans l'Observateur des événements Windows. Pour rechercher les événements relatifs à MSME dans l'Observateur des 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 **MSME** dans la colonne **Source**.
Ecrire les événements d'information	Permet de consigner les événements classés dans la catégorie **Informations**.
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 de la page **Paramètres et diagnostics** | **Journal du produit** en spécifiant les paramètres nécessaires à la génération de journaux du produit.

Procédure

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 5-17 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	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 : • **<Dossier d'installation>** : permet de créer le fichier journal du produit sous le répertoire d'installation de MSME. • **<Lecteur système>** : permet de créer le fichier journal du produit sous le répertoire `C:\Windows\system32`. • **<Fichiers programme>** : permet de créer le fichier journal du produit sous le répertoire `C:\Program Files (x86)` de Windows. • **<Dossier Windows>** : permet de créer le fichier journal du produit sous le répertoire `C:\Windows`. • **<Dossier de données>** : permet de créer le fichier journal du produit sous le répertoire `C:\ProgramData\`. • **<Chemin d'accès complet>** : permet de stocker le fichier journal du produit dans le chemin d'accès complet spécifié dans la zone de texte adjacente. 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.
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	Permet de spécifier un nom de fichier personnalisé pour le journal du produit. Le nom du fichier par défaut est `productlog.bin`, disponible sous le répertoire `<dossier d'installation>\Data\`. 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.
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	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. 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.
Limiter l'âge des entrées	Permet de supprimer les entrées du journal du produit après une période définie.
Age maximal de l'entrée	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 5-17 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**.

Configuration des paramètres du service 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

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 rapport d'erreurs**. Vous pouvez utiliser les options suivantes :

Tableau 5-18 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 exceptionnels tels que les blocages du système.
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.

Affichage des journaux du produit

Affichez l'état de fonctionnement du produit à l'aide des entrées du journal relatives aux événements, aux informations, aux avertissements et aux 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

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 A la section **Journal du produit**, vous pouvez utiliser les options suivantes :

Tableau 5-19 Définition des options

Option	Définition
ID	Permet d'indiquer le numéro servant à identifier une entrée spécifique du journal du produit. Par exemple, si vous souhaitez uniquement afficher les journaux du produit dont l'ID est supérieur à 2 000, spécifiez : `200*`
Niveau	Permet de sélectionner **Informations**, **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 : `*service*`
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.
Exporter vers un fichier .CSV	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. • 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.

3 Cliquez sur **Rechercher**.

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

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

Configuration des paramètres de fichiers DAT

Vous avez la possibilité de spécifier le nombre d'anciens fichiers DAT pouvant être gérés 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

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 L'option **Nombre maximal de fichiers DAT obsolètes** permet de spécifier le nombre maximal de générations de fichiers DAT à conserver sur le système lors des mises à jour régulières. MSME conserve les fichiers DAT les plus récents avec les anciens dans le répertoire `<dossier d'installation>\bin\DATs`. Lors de chaque nouvelle mise à jour de fichiers DAT, MSME 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.

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

Importation et exportation de paramètres de configuration

Définissez les paramètres destinés à exporter la configuration MSME existante (paramètres et stratégies compris) en vue de l'importer et de l'utiliser sur un autre serveur MSME. 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**. Dans la page **Importer et exporter des configurations**, les onglets suivants sont disponibles :

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

  Tableau 5-20 Onglet Configuration — Définition des options

Option	Définition
Exporter	Permet de copier la configuration de MSME (paramètres et stratégies) de ce serveur et de l'enregistrer à un emplacement où elle peut être importée par d'autres serveurs MSME. Le fichier de configuration MSME par défaut s'intitule `McAfeeConfigXML.cfg`.
Restaurer les valeurs par défaut	Permet de restaurer les paramètres MSME afin de rétablir les performances maximales du produit.
Restauration améliorée	Permet de restaurer les paramètres MSME afin de rétablir la protection maximale du produit.
Parcourir	Permet de localiser le fichier de configuration (`McAfeeConfigXML.cfg`) à importer.
Importer	Permet d'appliquer les paramètres d'un autre serveur MSME vers ce serveur. Par exemple, pour installer MSME 8.5 sur 5 systèmes : **1** Installez MSME sur le système 1. **2** Configurez les paramètres comme requis. **3** Exportez la configuration vers le fichier cfg. Pour plus d'informations sur l'importation de la configuration, voir l'étape 10 dans *Installer le logiciel à l'aide de l'assistant*. 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 MSME7.6 ou 8.0 vers un serveur MSME 8.5.

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

  Tableau 5-21 Onglet Liste de sites — Définition des options

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

Exportation d'une configuration MSME existante

Exportez la configuration d'un serveur MSME et enregistrez-la à un emplacement donné, à partir duquel d'autres serveurs MSME pourront l'importer ultérieurement.

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

Vous avez à présent terminé l'exportation de vos paramètres et stratégies MSME existants dans un fichier de configuration, que d'autres serveurs MSME pourront importer ultérieurement.

Importation d'une configuration à partir d'un autre serveur MSME

Appliquez les paramètres de configuration MSME d'un autre serveur sur ce serveur MSME.

Vous pouvez importer la configuration de deux manières différentes :

- Importer la configuration pendant l'installation du logiciel.
- Importer le fichier de configuration après l'installation du logiciel à l'aide de l'option **Importer et exporter la configuration** à partir de la page **Paramètres et diagnostics**.

- 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 MSME à partir d'un serveur MSME 7.6 vers un serveur MSME 8.0.
- Il est conseillé d'importer les paramètres entre serveurs MSME dotés du même rôle Exchange.

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. Cliquez sur l'onglet **Configuration**.
3. Dans la section **Importer une configuration**, cliquez sur **Parcourir** afin de localiser le fichier de configuration. Le fichier de configuration par défaut s'intitule `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 MSME vers ce serveur.

Importation d'une liste Sitelist

Importez des listes Sitelist qui spécifient 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, MSME utilise l'**éditeur SiteList** qui dirige vers une URL McAfee pour les mises à jour automatiques.

Si votre serveur MSME est managé par McAfee ePO, les mises à jour automatiques sont effectuées à l'aide de la liste Sitelist ePolicy Orchestrator. Si vous n'utilisez pas ePolicy Orchestrator pour gérer votre serveur MSME, créez un fichier Sitelist qui dirigera votre serveur MSME vers un référentiel local.

Il est possible de créer d'autres listes Sitelist à l'aide du logiciel McAfee AutoUpdate Architect ou de McAfee ePO.

Procédure

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 SiteList** sous **Démarrer** | **Tous les programmes** | **McAfee** | **Security for Microsoft Exchange** 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 proxy antispam

Configurez ces paramètres si votre organisation utilise un serveur proxy pour se connecter à Internet, afin que MSME puisse télécharger les règles antispam.

Le logiciel peut également utiliser ce proxy pour obtenir la réputation de l'adresse IP, la réputation des messages, et télécharger la base de données d'URL locale à partir du serveur GTI.

> Cette fonctionnalité s'applique uniquement si le composant de module complémentaire McAfee Anti-Spam est installé.

Procédure

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

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

2 Sélectionnez **Utiliser proxy**. Dans la section **Détails du serveur proxy**, vous pouvez utiliser les options suivantes :

Tableau 5-22 Définition des options

Option	Définition
Adresse IP	Permet de spécifier l'adresse IP du serveur proxy.
Port	Permet de spécifier le port utilisé pour les communications nécessitant un accès Internet.
Détails d'authentification	Permet de spécifier un type d'authentification. Vous pouvez utiliser les options suivantes : • **Anonyme** : permet d'accéder à l'ordinateur proxy sans préciser les détails d'authentification. • **NTLM** : permet d'accéder à l'ordinateur proxy à l'aide des informations d'identification de NT LAN Manager (NTLM). • **Authentification de base** : permet de fournir un **Nom d'utilisateur** et un **Mot de passe** pour que l'utilisateur accède à l'ordinateur proxy. Ressaisissez le mot de passe dans le champ **Confirmez le mot de passe**.

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

6 Maintenance du programme

Vous pouvez effectuer des tâches de maintenance produit telles que la modification de l'installation, la réparation, la désinstallation, la restauration des paramètres par défaut, la purge et l'optimisation de la base de données.

Sommaire

Modification de l'installation

Modifiez les fonctionnalités du programme MSME comme il convient et changez la manière dont les fonctionnalités du programme sont installées sur l'ordinateur ou suite à la modification du rôle serveur Exchange.

Vous pouvez également modifier l'installation de MSME à partir de la console **Panneau de configuration** | **Programmes et fonctionnalités** | **Désinstaller un programme** en cliquant sur **Désinstaller/Modifier**.

Procédure

1. Dans le dossier contenant les fichiers d'installation, double-cliquez sur `setup_x64.exe`.
2. Cliquez sur **Suivant** dans l'écran de bienvenue.

   L'écran **Maintenance du programme** s'affiche.
3. Sélectionnez **Modifier**, puis cliquez sur **Suivant**.
4. Sélectionnez les fonctionnalités du programme à modifier, puis cliquez sur **Suivant**.
5. Sélectionnez **J'accepte les termes de l'Accord de licence**, puis cliquez sur **Suivant**.
6. Cliquez sur **Installer** pour terminer l'installation en validant la modification des fonctionnalités du programme.
7. Une fois l'installation terminée, cliquez sur **Terminer**.

Restauration des paramètres par défaut

Restaurez la configuration par défaut du produit et bénéficiez de performances maximales.

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.

4 Cliquez sur **OK**.

Vous avez à présent terminé la restauration des paramètres de configuration par défaut du serveur MSME en vue d'optimiser les performances.

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** | **Eléments détectés**.

La page **Eléments 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 MSME. La valeur par défaut est **Chaque mois**.
- **Fréquence d'optimisation** : permet de récupérer l'espace disque occupé par les enregistrements de base de données supprimés. Selon la valeur attribuée à l'option **Age maximal de l'élément (jours)**, les anciens enregistrements seront supprimés si vous avez planifié une tâche de purge. Une fois les anciens enregistrements supprimés, MSME utilisera encore l'espace disque spécifié dans le champ **Seuil d'espace disque (Mo)**, même si la base de données de quarantaine n'a pas atteint la limite de taille. Afin d'optimiser et de réduire la base de données, planifiez une tâche d'optimisation. La valeur par défaut est **Chaque mois**.

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

3 Cliquez sur **Modifier la planification** afin de définir une nouvelle planification.

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

7 Dépannage

Identifiez et résolvez les problèmes rencontrés lors de l'utilisation de MSME. Familiarisez-vous avec les compteurs de performances disponibles et les clés de Registre importantes associés à ce produit.

Sommaire

Paramètres de configuration par défaut et améliorés

Selon les exigences de l'organisation, vous pouvez configurer MSME de manière à privilégier les performances ou la protection.

Pour modifier les paramètres de configuration de MSME, accédez à **Paramètres et diagnostics** | **Importer et exporter la configuration**. Vous pouvez utiliser les options suivantes :

- **Restaurer les paramètres par défaut** : permet de configurer MSME pour des performances optimales.
- **Restauration améliorée** : permet de configurer MSME pour une protection optimale.

Tableau 7-1 Différences entre les configurations par défaut et améliorée

Fonctionnalité	Configuration par défaut	Configuration améliorée
Réputation des messages	Désactivée	Activée
Réputation de l'adresse IP	Désactivée	Activée
Niveau d'imbrication maximal	10	50
Fichier protégé par mot de passe	Autoriser	Remplacer et mettre en quarantaine
Fichier protégé	Autoriser	Remplacer et mettre en quarantaine
Filtre des fichiers	Désactivé	Activé avec la règle par défaut (*.exe, *.com, *.bat, *.scr)
Fichier chiffré	Autoriser	Remplacer et mettre en quarantaine
Fichier corrompu	Autoriser	Remplacer et mettre en quarantaine
Réputation de l'URL de courrier	Désactivé	Activé uniquement pour les stratégies d'analyse à l'accès.

Clés de Registre importantes

Créez ces clés de Registre lorsque l'importance correspond à vos exigences.

Tableau 7-2 MSME — Clés de Registre importantes

Clé de Registre	Chemin d'accès	Importance
Nom : DigestMail Type : DWORD Valeur : 1	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\ADUserCache`	Gère un cache des alias utilisateur et des adresses SMTP, qui est utilisé lorsque MSME est intégré avec MQM et que la même adresse est utilisée pour la fonctionnalité E-mail de résumé.
Nom : ODUserID Type : REG_SZ Valeur : [Exemple : <admin@domaine.com>]	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\E2007`	Valide uniquement pour tous les serveurs de boîtes aux lettres Exchange. Doit être l'adresse e-mail de l'utilisateur à la demande créée par le produit et utilisée pour l'interaction avec les services web Exchange pour l'obtention des données d'e-mail en provenance de la base de données Exchange.
Nom : EWSUrl Type : REG_SZ Valeur : https://<adresse IP>/EWS/Exchange.asmx	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\OnDemand`	Valide uniquement pour les serveurs de boîtes aux lettres Exchange 2010. Il s'agit de l'URL utilisée pour la connexion aux services web Exchange hébergés par le serveur CAS. Cette valeur est renseignée par le script PowerShell GetHubTxDetails.ps1 pendant l'installation et à chaque redémarrage du service MSME.
Nom : SCLJunkThreshold Type : DWORD Valeur par défaut : 4	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Valide uniquement pour les serveurs de boîtes aux lettres Exchange 2010. Il s'agit du seuil de courrier indésirable SCL, qui est récupéré à partir d'AD et se situe au niveau de l'organisation. Tout score supérieur à cette valeur est traité comme du courrier indésirable, ce qui facilite l'acheminement de ce type de courrier sur les serveurs de transport Hub Exchange 2007/2010. Cette valeur est renseignée par le script PowerShell GetSCLJunkThreshold.ps1 lors de l'installation et par la suite, de manière périodique.
Nom : IPBlackList Type : REG_SZ Valeur : [Exemple : 10.0.0.1]	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState`	Bloque manuellement une adresse IP spécifique ou une plage d'adresses IP et empêche l'envoi d'e-mails à votre organisation à partir de cette ou de ces adresses, indépendamment de leur réputation.
Nom : SPFMaxTimeSec Type : DWORD Valeur par défaut : 5	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Durée maximale d'exécution du mécanisme SPF. Si cette durée dépasse la valeur définie, une *erreur temporelle* se produit et l'e-mail est livré.
Nom : SPFCacheTimeoutSec Type : DWORD Valeur par défaut : 43200	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Durée passée laquelle l'entrée de cache devient caduque. La durée par défaut est de 12 heures.
Nom : SPFCacheMaxEntries Type : DWORD Valeur par défaut : 5000	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Nombre maximum d'entrées dans le cache.

Tableau 7-2 MSME — Clés de Registre importantes *(suite)*

Clé de Registre	Chemin d'accès	Importance
Nom : SPFDNSTimeoutMS Type : DWORD Valeur par défaut : 1000	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Durée de chaque demande DNS, en millisecondes.
Nom : CacheTimeOutForNullRecords Type : DWORD Valeur par défaut : 60	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam`	Durée des enregistrements nuls (cas d'erreur temporelle), en secondes.

Les clés de registre SPFMaxTimeSec, SPFCacheTimeoutSec, SPFCacheMaxEntries, SPFDNSTimeoutMS et CacheTimeOutForNullRecords sont créées uniquement si vous avez installé le composant McAfee Anti-Spam ou le logiciel à l'aide de l'option d'installation complète.

8 Foire aux questions (FAQ)

Cette section fournit des réponses à des situations courantes, que vous êtes susceptible de rencontrer au cours de l'installation ou de l'utilisation du produit. Elle contient des informations de dépannage sous la forme de foire aux questions.

Pour afficher la liste à jour des questions associées à cette distribution, consultez l'article KB76886 dans McAfee KnowledgeBase.

Sommaire

Questions d'ordre général

La section qui suit présente des réponses aux questions fréquemment posées d'ordre général.

Est-il possible de définir des priorités pour la remise des e-mails ?

Non. Il n'est pas possible de définir des priorités, étant donné qu'il s'agit d'une tâche serveur Exchange.

Est-il toujours nécessaire d'activer l'accès anonyme au connecteur de réception du serveur Exchange ?

Non. MSME ne nécessite pas l'accès anonyme au connecteur de réception du serveur Exchange. Cette activité est la responsabilité de l'utilisateur à la demande. Pour plus d'informations sur la configuration des paramètres d'accès anonyme, consultez l'article KB81752 dans la base de connaissances McAfee KnowledgeBase.

Les e-mails analysés au niveau du serveur de transport Hub sont-ils analysés par le serveur de boîtes aux lettres ?

Cela dépend. Les e-mails analysés sur le serveur Hub et qui disposent de la même référence antivirus (AV) ne sont pas analysés au niveau du serveur de boîtes aux lettres. En revanche, ils le sont si la référence AV diffère en termes de fournisseur AV ou de version du moteur ou des fichiers DAT.

Pourquoi est-il nécessaire d'utiliser l'option Exécuter en tant qu'administrateur de Windows 2008 pour ouvrir l'interface utilisateur de MSME ?

Pour des raisons de sécurité, MSME ne peut pas communiquer avec les serveurs RPC. Ceci est dû au fait que le SID n'est pas autorisé à établir des communications interprocessus (IPC, Inter-Process Communication) avec le processus RPC.

Sous quel fichier exécutable les modules d'analyse de MSME sont-ils chargés dans toutes les versions d'Exchange ?

Le processus `RPCServ.exe` charge tous les fichiers binaires d'analyse. Pour identifier l'ID du processus de l'analyseur, consultez la ligne de commande du **Gestionnaire des tâches** et identifiez le processus `RPCServ.exe` doté du paramètre de ligne de commande /EVENTNAME:Global\MSME_scanner_RPCEvent.

Quelle est la configuration optimale de MSME ?

Les configurations possibles permettent de bénéficier d'une **protection optimale** ou de **performances optimales**. La configuration par défaut privilégie les performances.

Quels composants faut-il exclure si MSME et un programme antivirus de niveau fichier sont installés sur le même serveur ?

Excluez tous les dossiers et sous-dossiers binaires MSME, la base de données Postgres, les dossiers de réplication, les dossiers Exchange, le dossier d'événements McAfee ePO et le journal du produit.

Où puis-je trouver des informations complémentaires concernant la sécurisation de la messagerie ?

Pour en savoir plus sur les solutions de sécurisation de la messagerie, rendez-vous sur le site web http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx.

Comment puis-je accéder à l'interface produit du système distant ?

Pour accéder à l'interface autonome MSME distante :

1. Lancez **McAfee Security for Microsoft Exchange — Configuration du produit**.
2. A partir du menu **Changer de serveur**, cliquez sur **Nouvelle connexion**.
3. Dans la boîte de dialogue **Rechercher un ordinateur**, saisissez l'adresse IP du système distant, puis cliquez sur **OK**

Pour accéder à l'interface Web MSME distante :

1. Lancez **McAfee Security for Microsoft Exchange — Configuration du produit (interface Web)**.
2. Dans la barre d'adresse, saisissez : `https://<Remote system IP Address>/MSME/0409/html/index.htm`
3. Saisissez les informations d'identification de connexion lorsque vous y êtes invité.

Comment MSME se connecte-t-il au serveur TIE ?

MSME se connecte au serveur TIE via le client Data Exchange Layer (DXL) de McAfee ePO. Le serveur McAfee ePO qui gère MSME devrait également gérer le serveur TIE.

Comment puis-je configurer le serveur TIE dans MSME ?

Vous ne pouvez pas configurer le serveur TIE directement dans MSME. Toutefois, le serveur McAfee ePO qui gère MSME devrait également gérer le serveur TIE. Pour intégrer le serveur TIE dans McAfee ePO, reportez-vous au *Guide Produit de McAfee Threat Intelligence Exchange*.

Gestionnaire de stratégies

La section qui suit présente des réponses aux questions fréquemment posées concernant la fonctionnalité **Gestionnaire de stratégies**.

Comment créer et utiliser des stratégies e-mail ?

Veillez à toujours créer les stratégies sur des serveurs de passerelle en utilisant des adresses SMTP et sur des serveurs de boîtes aux lettres à l'aide de groupes Active Directory (AD). Sur le serveur de boîtes aux lettres, la conception de stratégies basées sur des adresses SMTP revient extrêmement cher, car le produit n'obtient pas les adresses SMTP et, pour résoudre ce problème, des requêtes AD sont effectuées. Cette procédure a pour effet de ralentir les performances sur les serveurs de boîtes aux lettres.

Les noms de domaine figurant dans les stratégies ont-ils un impact sur les performances ?

Yes. Pour une explication détaillée, consultez la question précédente, *Comment créer et utiliser des stratégies e-mail ?*.

Comment fonctionne le système de priorité des stratégies ?

Dès que la première stratégie enfant est satisfaite conformément à la priorité de résolution définie, la stratégie suivante n'est pas évaluée.

Est-il avantageux d'utiliser plusieurs stratégies et cela a-t-il un impact sur les performances du serveur ?

Oui, les performances s'en trouveront affectées. Lors de l'évaluation des stratégies, si la première stratégie enfant n'est pas satisfaite et que la stratégie suivante est évaluée, il se peut que des requêtes AD aient été émises, entraînant un ralentissement des performances.

Comment configurer MSME de manière à bloquer les fichiers exécutables à un niveau granulaire ?

Pour ce faire, utilisez l'option **Règles de filtrage de fichiers**. Par exemple, voyons comment filtrer des fichiers exécutables précis comme des fichiers exécutables Windows.

1. A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies** | **A l'accès (Stratégie principale)**.
2. Sous **Analyseurs noyaux**, cliquez sur **Filtrage des fichiers** et activez cette option.
3. Sous **Options (Paramètres antispam de base)**, cliquez sur **Modifier**.
4. Dans la liste déroulante **Règles disponibles**, sélectionnez **<Créer une nouvelle règle…>**.
5. Spécifiez un nom de règle, puis sous **Filtrage des catégories de fichiers**, sélectionnez **Activer le filtrage des catégories de fichiers**.
6. Dans la liste **Catégories de fichiers**, sélectionnez **Autres formats spécifiques**.
7. Dans la liste **Sous-catégories**, sélectionnez **Exécutables Windows**.
8. Cliquez sur **Enregistrer**.

Quels sont les types de fichier détectés comme programmes de compression ou programmes potentiellement indésirables (PUP), et à partir de quel paramètre est-il possible de contrôler cette fonctionnalité ?

Les programmes de compression et les programmes potentiellement indésirables (PUP) font partie de la catégorie de contenu malveillant détectée en fonction de la catégorie. Les programmes de compression correspondent généralement à des fichiers compressés ou zippés à l'aide d'un algorithme puis décompressés au moment de leur exécution.

Pour contrôler ce paramètre, accédez aux **Paramètres antivirus** disponibles dans l'interface utilisateur de MSME.

Paramètres et diagnostics

La section qui suit présente des réponses aux questions fréquemment posées concernant la fonctionnalité **Paramètres et diagnostics**.

L'activation de McAfee GTI provoque-t-elle une latence dans la remise des e-mails ?

Oui, la validation des e-mails par le service McAfee GTI entraîne une certaine latence.

Comment vérifier que l'analyseur du trafic recherche les e-mails de spam ?

Pour vérifier cette fonctionnalité, procédez à partir de l'interface utilisateur du produit de l'une des manières suivantes :

- A la page **Eléments récemment analysés**, consultez les e-mails analysés et la stratégie d'analyse utilisée. La mention **Passerelle** devrait figurer sous le champ **Analysé par**.
- Dans la base de données **Eléments détectés**, vérifiez l'absence d'e-mails de spam. Enfin, vérifiez que les e-mails n'ont pas été acheminés via des sessions authentifiées, ce qui est consigné sous **Journalisation de débogage** de MSME.

Est-il possible d'exporter les listes blanches et les listes noires d'un serveur MSME vers un autre ?

Oui, vous pouvez exporter les listes blanches et les listes noires d'un serveur MSME vers un autre. Pour ce faire :

1. A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies** | **Passerelle (Stratégie principale)**.
2. Sous **Analyseurs noyaux**, cliquez sur **Antispam**.
3. Sous **Options (Paramètres antispam de base)**, cliquez sur **Modifier**.
4. Cliquez sur l'onglet **Listes de courrier**, puis sur **Exporter** pour enregistrer tous les expéditeurs et destinataires bloqués et autorisés dans un fichier CSV.

Composant de module complémentaire McAfee Anti-Spam

La section qui suit présente des réponses aux questions fréquemment posées concernant le module complémentaire Anti-Spam.

Comment est-il possible de mettre à jour le moteur antispam manuellement ?

Mettez à jour la clé de Registre et placez le nouveau moteur dans le répertoire spécifié, indiqué dans le Registre sous la clé de Registre `SpamEngineVersion`, sous le Registre `MSME\SystemState`. Ces deux valeurs doivent être synchrones. Par exemple, si le moteur est doté de la version 9039, créez un répertoire intitulé `9039` sous `MSME\Bin\AntiSpam\Engine` et copiez le fichier du moteur `masecore.dll` dans ce répertoire.

Est-il possible de modifier manuellement les règles antispam ?

Non.

Quels sont les éléments à prendre en compte avant d'ajouter une adresse e-mail à la liste de blocage ?

- Assurez-vous que le composant de module complémentaire McAfee Anti-Spam est installé.
- Le serveur Microsoft Exchange doit être un serveur de transport. Par exemple, affectez à un serveur Exchange le rôle serveur de transport Edge ou serveur de transport Hub.
- Veillez à disposer d'une connexion sans authentification, au moyen de laquelle les e-mails atteignent directement le serveur depuis Internet.

Comment ajoute-t-on une adresse e-mail à la liste de blocage ou d'autorisation ?

1. A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies** | **Passerelle (Stratégie principale)**.
2. Sous **Analyseurs noyaux**, cliquez sur **Antispam**.
3. Sous **Options (Paramètres antispam de base)**, cliquez sur **Modifier**.
4. Cliquez sur l'onglet **Listes de courrier**, puis sur **Ajouter** en regard des options nécessaires telles que Expéditeurs bloqués, Expéditeurs autorisés, Destinataires bloqués ou Destinataires autorisés.

Que faire lorsque des e-mails ne sont pas détectés comme des messages de spam ?

Sous **Paramètres et diagnostics** | **Antispam**, sélectionnez **Activer la réputation des messages** et appliquez les paramètres. Ajustez également le score de spam en lui attribuant une valeur comprise entre 51 et 79, ce qui améliorera le taux de détection.

Les e-mails dotés d'un score de spam inférieur (compris entre 51 et 59) peuvent néanmoins être légitimes. C'est pourquoi il est nécessaire de rectifier encore le score.

Comment obtient-on une licence pour le module complémentaire Anti-Spam ?

Vous pouvez télécharger le fichier `MSMEASA.ZIP` à partir du site de téléchargement McAfee si vous disposez d'un numéro Grant Number McAfee Anti-Spam valide. Si vous ne possédez pas ce numéro, contactez l'équipe du Service Client McAfee.

Expressions régulières

La section qui suit présente des réponses aux questions fréquemment posées concernant les expressions régulières (regex).

L'activation des expressions régulières entraîne-t-elle une latence au niveau des e-mails ?

Oui, l'activation des expressions régulières entraîne une latence au niveau des e-mails, car l'analyse du contenu est une configuration qui mobilise énormément les processus.

Où puis-je trouver des informations complémentaires sur les expressions régulières ?

Différents sites web présentent des informations sur les expressions régulières.

En voici quelques uns :

- http://www.regular-expressions.info/reference.html
- http://www.regexbuddy.com/regex.html

Comment bloquer certains numéros de carte de crédit et de numéros de sécurité sociale à l'aide d'expressions régulières ?

1. A partir de l'interface utilisateur du produit, cliquez sur **Gestionnaire de stratégies** | **Ressource partagée**. La page **Ressources partagées** s'affiche.
2. Sous l'onglet **Dictionnaires de conformité et DLP**, cliquez sur **Nouvelle catégorie** et spécifiez un nom de catégorie.
3. Cliquez sur **OK**.
4. Sous **Règles de conformité et DLP**, cliquez sur **Créer une nouvelle catégorie**.

5 Renseignez les champs **Nom de la règle** et **Description**, puis spécifiez l'expression régulière dans le champ **Terme ou phrase**.

Tableau 8-1 Exemple : procédure de validation de numéros de carte de crédit

Type de carte	Expression régulière	Description
Visa	`^4[0-9]{12}(?:[0-9]{3})?$`	Tous les numéros de carte Visa commencent par le chiffre 4. Les nouvelles cartes comprennent 16 chiffres. Les anciennes cartes en comptaient 13.
MasterCard	`^5[1-5][0-9]{14}$`	Tous les numéros MasterCard commencent par les nombres 51 à 55. Tous comprennent 16 chiffres.
American Express	`^3[47][0-9]{13}$`	Les numéros de carte American Express commencent par 34 ou 37 et comptent 15 chiffres.
Diners Club	`^3(?:0[0-5]|[68][0-9])[0-9]{11}$`	Les numéros de carte Diners Club commencent par 300 à 305, 36 ou 38. Tous comptent 14 chiffres. Certaines cartes Diners Club commencent par un 5 et comportent 16 chiffres. Il s'agit de numéros d'association entre Diners Club et MasterCard, qui doivent être traités comme des numéros MasterCard.
Discover	`^6(?:011|5[0-9]{2})[0-9]{12}$`	Les numéros de carte Discover commencent par 6011 ou 65. Tous comptent 16 chiffres.
JCB	`^(?:2131|1800|35\d{3})\d{11}$`	Les cartes JCB qui commencent par 2131 ou 1800 comprennent 15 chiffres. Les cartes JCB commençant par 35 comptent 16 chiffres.

Vous pouvez vous inspirer de l'exemple ci-dessus pour créer une expression régulière similaire applicable aux numéros de sécurité sociale. Pour prendre connaissance d'autres exemples d'expressions régulières, visitez le site web http://www.regular-expressions.info/examples.html.

6 Sélectionnez l'option **Expression régulière**, puis cliquez sur **Enregistrer**.

7 Ajoutez cela à la stratégie **Conformité et DLP** dans le **Gestionnaire de stratégies**. Pour ce faire, cliquez sur **Gestionnaire de stratégies | A l'accès (Stratégie principale) | Conformité et DLP**.

8 Sous **Activation**, sélectionnez **Activer**.

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

10 Sous **Sélectionner un groupe de règles**, sélectionnez dans la liste déroulante la règle d'expression régulière créée précédemment.

11 Spécifiez l'action à entreprendre suite au déclenchement de la règle.

12 Cliquez sur **Enregistrer**.

Index

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V