Guide produit

Customer Submission Tool

Version 2.0

McAfee®
Protection système

Solutions de pointe du marché en matière de prévention des intrusions

McAfee®

Sommaire

1 Introduction

McAfee Customer Submission Tool réduit le nombre de *spams* reçus dans la messagerie Microsoft® Outlook®. Il transfère ces e-mails indésirables directement aux laboratoires McAfee ou à d'autres produits McAfee capables d'analyser les échantillons à des fins d'apprentissage.

Cette section aborde les points suivants :

Fonctions du produit

McAfee Customer Submission Tool prend en charge :

- Secure Content Management (SCM)
- McAfee Quarantine Manager (MQM)

Dans le client Microsoft Outlook, l'outil ajoute des boutons de barre d'outils et des éléments de menu, et permet :

- de soumettre aux laboratoires McAfee les échantillons à analyser ;
- de soumettre à McAfee Quarantine Manager ou à Secure Content Management les échantillons utilisés à des fins d'apprentissage ;
- de soumettre les e-mails indésirables non identifiés comme étant des spams ou des hameçons ;
- de soumettre les e-mails identifiés à tort comme étant des spams ou des hameçons ;
- de supprimer éventuellement les messages soumis ;
- d'ajouter une adresse dans la liste de blocage et d'intercepter ainsi les futurs messages du spammeur ;
- d'ajouter une adresse dans la liste d'autorisation et d'éviter ainsi d'identifier à tort les futurs messages de l'expéditeur comme étant des spams ou des hameçons ;

- d'ajouter les adresses du dossier de contacts Microsoft Outlook à la liste d'autorisation et d'éviter ainsi d'identifier à tort les expéditeurs connus comme étant les auteurs de spams ou d'hameçons.

Pour installer l'outil, vous pouvez vous servir d'un assistant. Si vous destinez le produit à plusieurs utilisateurs e-mail, vous disposez d'un script.

Nouveautés de cette version

Cette version de Customer Submission Tool inclut les nouvelles fonctions et améliorations suivantes :

Facilitation de l'accès à l'outil

Version précédente	Pendant l'affichage des objets, des boutons sont disponibles dans la barre d'outils standard et des éléments le sont dans le menu **Actions**.
Version actuelle	Pendant l'affichage d'un e-mail, des boutons sont également disponibles dans la barre d'outils standard et des éléments le sont dans le menu **Actions**.
Avantages	Davantage de fonctions sont disponibles dans Microsoft Outlook.
Pour plus d'informations	Reportez-vous à la section *Utilisation du logiciel, page 23*.

Augmentation des destinataires de soumission

Version précédente	Pour améliorer le taux de détection de ses produits antispam, McAfee peut analyser les e-mails mal identifiés une fois soumis aux laboratoires McAfee.
Version actuelle	Vous pouvez également soumettre les e-mails à : ■ McAfee Secure Content Management ■ McAfee Quarantine Manager
Avantages	Les échantillons permettent aux bases de données bayésiennes de mieux reconnaître des spams, des hameçons ou des messages acceptables.
Méthode d'accès	Cette fonction est disponible si l'outil est installé ou configurable ultérieurement.
Pour plus d'informations	Reportez-vous à la section *Utilisation du logiciel, page 23*.

Utilisation automatique de listes de blocage et d'autorisation

Version précédente	Cette fonction n'était pas disponible.
Version actuelle	Cette fonction est disponible si vous utilisez l'outil avec McAfee Quarantine Manager (MQM). Grâce à elle, vous pouvez ajouter automatiquement des adresses e-mail à une liste d'autorisation (en cas d'expéditeurs fiables) ou de blocage (en présence de spammeurs reconnus). En un clic, vous êtes à même d'y inclure les contacts Microsoft Outlook.
Avantages	Contrairement aux futurs e-mails de spammeurs identifiés, les prochains messages d'expéditeurs autorisés ne seront pas considérés comme des menaces.
Méthode d'accès	Cette fonction est disponible si un e-mail est soumis à MQM à des fins d'analyse.
Pour plus d'informations	Reportez-vous à la section *Ajout de vos contacts Microsoft Outlook à la liste d'autorisation, page 27*.

Non-limitation du nombre de soumissions

Version précédente	Vous ne pouviez soumettre que 10 échantillons à la fois.
Version actuelle	Ce nombre limite ne s'applique pas.
Avantages	Il est plus rapide et facile de soumettre des e-mails.

Suppression automatique après la soumission

Version précédente	Après soumission, vous deviez supprimer manuellement les spams ou les hameçons.
Version actuelle	Vous pouvez choisir de supprimer chaque e-mail sélectionné immédiatement après soumission.
Avantages	Il est plus rapide et facile de soumettre des e-mails.

Utilisation de ce guide

Ce guide fournit des informations sur la configuration et l'utilisation du produit. Il contient les chapitres suivants :

- *Introduction*
  Présentation du produit, incluant la description des fonctionnalités nouvelles ou modifiées. Présentation du guide. Informations de contact McAfee.
- *A propos des spams et des hameçons*
  Informations sur les spams/hameçons et moyen de limiter leur nombre.
- *Installation du logiciel*
  Téléchargement des fichiers. Utilisation d'un programme d'installation Microsoft Windows. Mise en place à l'aide d'un script.
- *Utilisation du logiciel*
  Mode de soumission des échantillons et de configuration de l'outil.

Public visé

Ces informations sont principalement destinées à deux types de personnes :

- Les administrateurs réseau responsables de la sécurité des messageries de leur société.
- Les utilisateurs chargés de configurer les options de détection.

Conventions

Ce guide utilise les conventions suivantes :

Gras condensé — Tous les termes issus de l'interface utilisateur, notamment les options, menus, boutons et noms des boîtes de dialogue.

Exemple
Renseignez les champs **Nom d'utilisateur** et **Mot de passe** du compte approprié.

`Courier` — Chemin d'un dossier/d'un programme ou texte saisi, notamment une commande à l'invite du système.

Exemples
L'emplacement par défaut du programme est :

```
C:\Program Files\McAfee\EPO\3.5.0
```

Exécutez la commande suivante sur l'ordinateur client :

```
scan --help
```

Italique — Elément mis en valeur ou nouveau terme, notamment en cas de titres de documentations et de sections.

Exemple
Pour plus d'informations, reportez-vous au *Guide produit de VirusScan Enterprise*.

Bleu — Lien actif et/ou adresse Web (URL).

Exemple
Consultez le site Web de McAfee à l'adresse :

`http://www.mcafee.com`

<TERME(S)> — Les chevrons signalent un terme générique.

Exemple
Dans l'arborescence de la console, cliquez avec le bouton droit sur <SERVEUR>.

Remarque : information complémentaire (par exemple, un autre moyen d'exécuter la même commande).

Astuce : utilisation optimale/recommandation de McAfee en matière de prévention des menaces, de performances et d'efficacité.

Attention : conseil important sur la protection de votre système informatique, de votre entreprise, de votre installation logicielle ou de vos données.

Avertissement : mise en garde d'un utilisateur contre les blessures corporelles liées à l'utilisation d'un produit matériel.

Obtention d'informations sur le produit

Sauf indication contraire, la documentation produit est proposée sous forme de fichiers au format .PDF. Elle est disponible sur le site de téléchargement de McAfee.

Guide produit : présentation du produit et de ses fonctions, instructions détaillées d'installation et de configuration du logiciel, informations sur le déploiement, les tâches répétitives et les procédures d'utilisation.

Notes de version : *readme*. Informations sur le produit, liste des problèmes résolus/connus et ajouts/changements de dernière minute apportés au produit ou à sa documentation. Un fichier texte est inclus dans l'application logicielle.

Accord de licence : document McAfee sur tous les types d'autorisation disponibles pour le produit concerné. Cet accord définit les conditions générales d'utilisation du logiciel sous licence.

Contacts : coordonnées des services et ressources McAfee - support technique, service clientèle, siège de la sécurité AVERT, programme bêta et formation. Un fichier texte est inclus dans l'application logicielle.

Contacts

Siège de la sécurité : AVERT

Page d'accueil
http://www.mcafeesecurity.com/us/security/home.asp

Bibliothèque d'informations sur les virus
http://vil.mcafeesecurity.com

Envoi d'un échantillon via AVERT WebImmune *(informations de connexion requises)*
https://www.webimmune.net/default.asp

Service AVERT de notification de fichiers DAT
http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Site de téléchargement

Page d'accueil
http://www.mcafeesecurity.com/us/downloads/

Mises à jour des fichiers DAT et du moteur antivirus
http://www.mcafeesecurity.com/us/downloads/updates/default.asp
ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x

Mises à jour des fichiers de règles et du moteur antispam
ftp://ftp.mcafee.com/spamdefs/1.x/

Mises à niveau du produit *(informations de connexion requises)*
https://secure.nai.com/us/forms/downloads/upgrades/login.asp

HotFix et patch destinés aux vulnérabilités de sécurité *(accessibles à tous)*
http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp

HotFix et patch destinés aux produits *(compte ServicePortal et numéro de licence McAfee requis)*
https://mysupport.nai.com/products/products.asp

Support du produit en fin de vie
http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Support technique logiciel et matériel

Page d'accueil
http://www.mcafeesecurity.com/us/support/technical_support

Recherche dans la Base de connaissances (KnowledgeBase)
http://knowledgemap.nai.com/

McAfee Support technique ServicePortal *(informations de connexion requises)*
http://www.mcafeesecurity.com/us/support/

McAfee Security Alerting Service (MSAS)
http://mysupport.nai.com/supportinfo/psvans_info.asp

Service clientèle

E-mail
https://secure.nai.com/us/forms/support/request_form.asp

Site Web
http://www.mcafeesecurity.com/us/support/default.asp

Téléphone (numéro vert pour les Etats-Unis, le Canada et l'Amérique latine)
+1-888-VIRUS NO ou **+1-888-847-8766** du lundi au vendredi, de 8 h à 20 h (heure du Centre).

Coordonnées des bureaux internationaux de McAfee :
http://www.mcafeesecurity.com/us/contact/home.htm

Programmes bêta de McAfee

http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm

Formation : McAfee University

http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

2 A propos des spams et des hameçons

Méthode utilisée par le logiciel pour en réduire le nombre

Cette section décrit l'action du logiciel, ainsi que la façon dont il fonctionne avec les autres produits de sécurité McAfee pour réduire le nombre de spams.

Quelques termes utiles

Les définitions suivantes peuvent être utiles

- **Faux négatif** : e-mail qui n'a pas été considéré comme un spam ou un hameçon, mais qui en est généralement un.
- **Faux positif** : e-mail qui a été classé dans la catégorie des spams ou des hameçons, mais que le destinataire ne considère pas comme tel.
- **Spammeur** : personne ou organisation à l'origine de spams.
- **Usurpation** : par exemple, lorsque l'on falsifie l'origine d'un e-mail pour masquer l'identité de l'expéditeur dans le but de créer un site Web qui a l'air authentique.
- **Liste d'autorisation** : liste d'expéditeurs approuvés.
- **Liste de blocage** : liste d'expéditeurs qui envoient des spams ou des hameçons.

Qu'est-ce qu'un spam ?

Tout e-mail non sollicité et importun peut être considéré comme un spam. Sont inclus dans cette catégorie les messages commerciaux, l'équivalent électronique du *courrier publicitaire* ou les messages n'ayant aucun caractère commercial mais qui sont indésirables, comme les canulars, les blagues et les chaînes de lettres.

Il arrive fréquemment que, pour masquer leur véritable identité, les auteurs de spams, communément appelés *spammeurs*, falsifient les en-têtes des e-mails de façon à détourner les éventuelles mesures de répression vers des personnes innocentes.

Qu'est-ce qui n'est pas considéré comme un spam ?

Certains e-mails sont qualifiés de "spam" alors qu'ils n'en sont pas. Par exemple, si vous vous êtes abonné à une lettre d'informations ou inscrit sur un forum en ligne, ou si vous avez demandé des informations sur un produit ou récemment quitté un groupe de travail, votre adresse e-mail figure peut-être encore sur une liste de diffusion. Si vous souhaitez recevoir moins d'e-mails indésirables de ce type, supprimez votre adresse e-mail de toute ancienne liste de diffusion.

Comment faire pour ne plus recevoir de spams ?

Chaque fois que vous utilisez votre adresse e-mail pour envoyer des messages ou y répondre, envoyer des posts sur des forums de discussion ou faire connaître une adresse e-mail, vous exposez votre compte de messagerie aux *spammeurs*. Les spammeurs compilent des listes d'adresses e-mail. Plus le temps passe, plus le nombre de listes de réseaux de spammeurs auxquelles sont ajoutées ces adresses est important et plus vous recevez de spams.

Pour prendre de bonnes habitudes, vous devez suivre toutes les recommandations de votre société lorsque vous utilisez la messagerie. De cette façon, vous devriez recevoir moins de spams. Par exemple :

- **Prenez garde à ne pas acheter de produits plébiscités par des spams !** En effet, le spammeur serait ainsi au courant que l'adresse e-mail est active et celle-ci serait ensuite vendue à d'autres spammeurs. Ceci est également un moyen de vous obliger à révéler des données confidentielles.
- **Ne donnez pas votre adresse e-mail personnelle lorsque vous êtes en ligne.** Utilisez plutôt une adresse *secondaire* lorsque vous participez à des groupes de discussion, à des concours ou chaque fois qu'un tiers vous demande votre adresse e-mail. Si vous recevez trop de spams à cette adresse, vous pourrez cesser de l'utiliser et en créer une autre.
- **Ne répondez pas aux spams, même s'ils vous proposent de supprimer votre adresse de la liste de diffusion.** En effet, votre réponse indique au spammeur que l'adresse e-mail est active et celle-ci peut ensuite être vendue à d'autres spammeurs.

Vous pouvez également consulter la section *Notion de scores de spams, page 15* afin de mieux comprendre comment une configuration prudente des produits anti-spam de McAfee peut vous éviter de recevoir des spams.

Qu'est-ce qu'un hameçon ?

Certains spammeurs se spécialisent dans les messages d'*usurpation*, dont le but est de piéger des utilisateurs peu méfiants en leur faisant révéler des informations sur leur identité et sur leurs comptes bancaires. Ce type de spam est appelé *hameçonnage*.

Dans la plupart des cas, vous recevez un e-mail qui semble provenir d'un organisme honnête, tel qu'une banque. Cet e-mail vous dirige en général vers un site Web *usurpé* où vous êtes invité à entrer vos informations confidentielles et bancaires telles que votre numéro de compte, votre mot de passe, votre numéro de carte de crédit et votre numéro de sécurité sociale. Les spammeurs peuvent ensuite utiliser l'identité dérobée pour obtenir des biens et des services de manière frauduleuse (tels que des prêts personnels) pour vous voler directement sur votre compte, ouvrir des comptes bancaires et blanchir de l'argent.

Comment faire pour ne plus recevoir d'hameçons ?

- **Méfiez-vous de tous les e-mails qui vous invitent à entrer vos mots de passe et autres informations confidentielles.** Les banques ne demandent jamais ce genre d'informations directement et les vérifient en général par courrier postal. Les organismes n'ont pas pour habitude de *perdre* les informations relatives à vos comptes. La procédure normale est que ce sont eux qui vous envoient vos nouvelles données par la Poste : ce n'est pas à vous de fournir ces informations par e-mail ou sur un site Web.

- **Méfiez-vous des liens vers des sites Web.** Lorsque vous êtes invité à fournir des informations confidentielles, vous pouvez être redirigé via un lien *usurpé*. Par exemple, un lien figurant dans un e-mail semble correspondre à l'adresse du site de votre banque (www.exemple.com) et vous connecte à un site qui a l'air authentique. Pourtant, l'adresse du navigateur affiche un nom différent (tel que www.exemple.net) ou une autre adresse IP (telle que 168.192.255.200).

- **Méfiez-vous des sites Web non sécurisés.** Les organismes légaux ont des sites Web sécurisés qui cryptent vos données confidentielles avant de les envoyer. Ils ont des adresses du type https://www.exemple.com plutôt que http://www.exemple.com. En d'autres termes, ils utilisent un protocole Internet sécurisé appelé **https** plutôt que **http**.

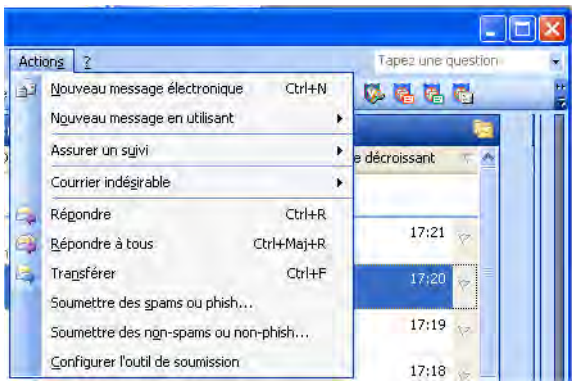
Qu'est-ce que le logiciel Customer Submission Tool ?

Les produits anti-spam constituent une protection fiable contre les spams. Toutefois, il est parfois difficile de détecter les spams ; les spammeurs développent de nouvelles techniques et les nouveaux spams ne sont détectés par *aucun* anti-spam. En outre, il arrive qu'il y ait des erreurs de détection : un anti-spam peut classer par erreur des messages inoffensifs dans la catégorie des spams.

En analysant les nouveaux spams (et les hameçons) et les e-mails mal classés, McAfee ne cesse d'améliorer ses produits anti-spam.

Le logiciel Customer Submission Tool fonctionne avec la messagerie Microsoft Outlook pour que vous receviez moins d'e-mails indésirables ou de *spams*. Des boutons et des entrées de menu supplémentaires s'affichent lorsque vous lisez un e-mail.

Figure 2-1 Boutons et menus supplémentaires dans Microsoft Outlook



L'outil peut soumettre des e-mails aux laboratoires McAfee ou à d'autres logiciels anti-spam de McAfee pour qu'ils soient analysés :

- **Envoi d'e-mails aux laboratoires McAfee**
  Nous sommes désireux d'améliorer constamment le système de détection de nos anti-spam. Pour cela, nous examinons les e-mails qui ont été classés à tort dans la catégorie des spams par nos logiciels ou par des produits d'autres fournisseurs, et nous essayons de savoir *pourquoi*.

  Tous les échantillons que vous nous soumettez sont considérés comme des données confidentielles ; nous ne les transmettons à personne et nous ne les utilisons pas à d'autres fins que la recherche. Pour analyser l'échantillon correctement, nous nous intéressons à l'en-tête du message, y compris à l'expéditeur et à l'objet, et au contenu, à savoir le texte et les pièces jointes éventuelles. Une déclaration de confidentialité complète s'affiche lorsque vous installez le logiciel.

- **Envoi d'e-mails à la solution Secure Content Management (SCM)**
  Si le réseau est protégé par une solution SCM, vous pouvez soumettre des échantillons à cette solution pour l'apprentissage bayésien. Reportez-vous à la page 15.

- **Envoi d'e-mails à McAfee Quarantine Manager (MQM)**
  Si le logiciel MQM est installé sur le réseau, vous pouvez soumettre des échantillons à McAfee Quarantine Manager pour l'apprentissage bayésien. Reportez-vous à la page 15.

Apprentissage bayésien

Les solutions Secure Content Management (SCM) et McAfee Quarantine Manager (MQM) ont recours à une base de données qui utilise la théorie de la probabilité de Bayes pour déterminer si un e-mail est un spam (ou un hameçon).

Vous pouvez apprendre à la base de données à reconnaître de nouveaux types de spams et d'hameçons en envoyant des échantillons à l'administrateur de SCM ou MQM. Une seule solution McAfee Quarantine Manager peut former plusieurs SCM.

Le logiciel Customer Submission Tool permet d'envoyer des échantillons d'un seul clic. L'administrateur peut ensuite décider quel échantillon il soumet à la base de données. Le logiciel analyse le contenu de chaque échantillon et *retient* les expressions de type spam pour les prochaines fois.

De la même manière, si vous recevez des e-mails qui ont été classés par erreur dans la catégorie des spams ou des hameçons, vous pouvez les envoyer à l'administrateur pour que le logiciel se souvienne qu'il ne s'agit pas de spams.

Plus vous soumettrez d'échantillons pour enrichir la base de données, plus vous aurez de chances que les spams et les hameçons soient classés dans la bonne catégorie à l'avenir.

Notion de scores de spams

Nos produits anti-spam testent un grand nombre de règles sur chaque e-mail. Chaque règle attribue une note positive ou négative au message. Les règles qui permettent de détecter des caractéristiques de spam valent au message une note positive. Celles qui permettent de détecter des attributs de messages légitimes octroient au message une note négative. Une fois additionnées, ces notes permettent d'attribuer à chaque message un *score de spam* global. Certaines règles sont simples et ne concernent que des expressions très courantes. D'autres, plus complexes, examinent les informations d'en-tête et la structure des e-mails.

Les produits anti-spam permettent de définir un seuil au-delà duquel l'e-mail sera considéré comme un spam. Généralement, un score de 5 indique qu'un e-mail est un spam. Vous pouvez configurer votre anti-spam de manière à ce qu'il mette en évidence ces e-mails en ajoutant du texte, par exemple **SPAM**, dans l'objet de l'e-mail. L'identification du spam étant ainsi facilitée, vous pouvez alors décider de lire ou non l'e-mail.

Il est important que vous configuriez votre anti-spam correctement pour qu'il classe les e-mails dans la catégorie des spams lorsque leur score dépasse un seuil prédéfini. Si ce seuil est trop élevé (un score de 10 ou plus), l'anti-spam ne considérera pas l'e-mail comme un spam. S'il n'est pas assez élevé, des e-mails inoffensifs risquent d'être considérés à tort comme des spams.

3 Installation du logiciel
(utilisateurs avancés et administrateurs)

Cette section présente l'installation de Logiciel Customer Submission Tool version 2.0. Elle aborde les points suivants :

Si vous destinez l'outil à plusieurs utilisateurs e-mail, nous vous recommandons d'utiliser un script. Reportez-vous à la section *Installation de l'outil à l'aide d'un script, page 19*.

Liste de contrôle d'installation

Pour obtenir Customer Submission Tool, vous pouvez le télécharger depuis notre site Web. Avant d'installer Customer Submission Tool, consultez la liste de contrôle ci-dessous. Ainsi, vous vous assurerez de disposer d'une configuration système correcte et de toutes les informations nécessaires à l'opération.

- ✓ L'ordinateur fonctionne sous Windows 2000 ou une version ultérieure.
- ✓ Les derniers Service Packs et mises à jour Microsoft ont été installés.
- ✓ Outlook 2000 ou une version ultérieure est installé. Sous Customer Submission Tool, d'autres clients de messagerie ne sont pas pris en charge, notamment Microsoft Outlook Express.
- ✓ L'ordinateur peut accéder aux fichiers d'installation téléchargés depuis le site Web de McAfee.
- ✓ Vous disposez des droits et des autorisations administrateur nécessaires à l'installation de Customer Submission Tool.

✓ Pour soumettre des e-mails à McAfee Quarantine Manager, préparez :

- le nom ou l'adresse IP du serveur MQM (par exemple, serveur1.domaine1 ou 192.168.255.200) ; le protocole HTTP ou HTTPS est utilisable.

En fonction du processus d'authentification, vous pouvez également nécessiter :

- le nom d'utilisateur requis pour l'accès direct à MQM (par exemple, utilisateur_réseau@exemple.com) ;
- le mot de passe correspondant.

✓ En l'absence du logiciel MQM, vous pouvez soumettre des e-mails à une solution Secure Content Management. Pour ce faire, préparez :

- Le nom ou l'adresse IP du serveur SMTP (par exemple, serveur1.domaine1 ou 192.168.255.200).

  La solution ne sera probablement pas directement accessible depuis un poste de travail. En général, cette adresse se rapporte donc au relais SMTP destiné au transfert des e-mails vers SCM. Il peut s'agir du serveur Microsoft Exchange.
- Port du serveur SMTP.
- Adresse e-mail de soumission des spams ou hameçons ignorés.
- Adresse e-mail de soumission des non-spams ou non-hameçons.

Téléchargement des fichiers d'installation

1. Créez un dossier temporaire sur votre disque dur.
2. Pour accéder à la page des produits antispam, consultez le site Web de McAfee à l'adresse suivante : http://www.mcafeesecurity.com/us/products/mcafee/antispam/category.htm.
3. Cliquez sur le lien **Outil de soumission de spam**, puis copiez l'archive dans le dossier temporaire. Pour décompresser le fichier .zip, vous pouvez obtenir de la plupart des services électroniques l'utilitaire nécessaire.

Installation manuelle de l'outil

Si vous destinez l'outil à plusieurs utilisateurs e-mail, nous vous recommandons d'utiliser un script. Reportez-vous à la page 19.

1 Fermez toutes les applications en cours.

2 A l'emplacement temporaire de téléchargement, double-cliquez sur le dossier de l'outil **McAfee Customer Submission Tool**.

3 Pour lancer l'assistant d'installation, exécutez MCST.EXE.

Si le programme d'installation ne sélectionne pas automatiquement la langue appropriée, vous pouvez la choisir dans la boîte de dialogue ouverte.

Figure 3-1 Boîte de dialogue de l'Assistant d'installation

4 Cliquez sur **Suivant** pour afficher la boîte de dialogue **Dossier de destination**.

5 Conservez l'emplacement par défaut ou indiquez un autre dossier d'installation à l'aide du bouton **Parcourir**, puis cliquez sur **Suivant**.

6 Dans la boîte de dialogue **Prêt pour l'installation de l'application**, cliquez sur **Suivant**. La boîte de dialogue **Mise à jour du système** s'affiche.

Elle présente des messages et une barre d'avancement. La copie des fichiers et l'installation du logiciel peuvent durer quelques minutes. Une fois le processus terminé, la boîte de dialogue **McAfee Customer Submission Tool a été installé correctement** s'affiche.

7 Cliquez sur **Terminer** pour fermer l'assistant.

8 Lancez Microsoft Outlook. Dans la barre d'outils standard du client de messagerie, des boutons supplémentaires sont disponibles. Reportez-vous à la figure 2-1, page 14.

Installation de l'outil à l'aide d'un script

Si vous comptez installer Customer Submission Tool sur plusieurs ordinateurs, nous vous recommandons d'utiliser un script. Pour télécharger les fichiers requis, reportez-vous à la section *Téléchargement des fichiers d'installation, page 17*.

En général, la commande d'installation a la forme suivante :

```
msiexec /qn /I mcst.msi paramètre1 paramètre2 paramètre3
```

Pour plus d'informations sur le programme d'installation de Windows, consultez le site Web de Microsoft.

Dans cette commande, les fonctions définissables lors de la configuration manuelle de l'outil peuvent servir de paramètres. Pour plus d'informations, reportez-vous à la section *Configuration du logiciel, page 27*.

Par ailleurs, les paramètres sont décrits dans les tableaux suivants.

Tableau 3-1 Paramètres généraux

Paramètre et valeur par défaut		Description
CONFIGENABLED	1 (Oui)	Affiche le bouton **Configurer les paramètres de soumission**. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 1.
DELETESPAMONSUBMIT	0 (Non)	Supprime les spams ou hameçons une fois soumis. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
DONTSHOWSPAMSUBMIT	0 (Non)	Masque la boîte de dialogue de soumission après envoi d'un spam ou hameçon. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
DONTSHOWHAMSUBMIT	0 (Non)	Masque la boîte de dialogue de soumission après envoi d'un e-mail mal identifié. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
INSTALLDIR1	Texte.	Installe l'outil à l'emplacement défini. Par défaut, le dossier d'installation est : « C:\Program Files\McAfee\Submission Tool »
MAXSUBMISSIONCOUNT	10000	Permet à l'utilisateur de soumettre simultanément de nombreux messages. Si la valeur dépasse le nombre limite, elle est considérée comme étant égale à 10 000.
REBOOT	(Aucun)	Redémarre le système d'exploitation à la fin de l'installation. Les paramètres utilisables sont : F = forcé, S = supprimer (recommandé) ou R = supprimer définitivement (recommandé).

Tableau 3-2 Paramètres de soumission aux laboratoires McAfee

Paramètre et valeur par défaut		Description
ASEENABLED	1 (Oui)	Active la soumission des échantillons aux laboratoires McAfee.
ASERESPONSEFREQ	0 (Immédiate-ment)	Fréquence de réponse des laboratoires McAfee aux soumissions. Les paramètres utilisables sont : 0 = **immédiatement**, 1 = **une fois/jour**, 2 = **une fois/semaine** ou 3 = **jamais**. Toute autre valeur est considérée comme étant égale à 0.
ASERESPONSETYPE	0 (Résumé)	Type de réponse des laboratoires McAfee. Les paramètres utilisables sont : 0 = **résumé**, 1 = **normal** ou 2 = **détaillé**. Toute autre valeur est considérée comme étant égale à 0.

Tableau 3-3 Paramètres de soumission à McAfee Quarantine Manager

Paramètre et valeur par défaut		Description
MQMENABLED	0 (Non)	Active la soumission des échantillons à MQM. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
MQMPATH « http://mqm.exemple.com/mqmuserui »		URL du dossier utilisateur sur MQM.
WHITELISTHAMONSUBMIT	0 (Non)	Ajoute automatiquement l'adresse de l'expéditeur dans la liste d'autorisation si l'e-mail soumis n'est ni un spam ni un hameçon. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
BLACKLISTSPAMONSUBMIT	0 (Non)	Ajoute automatiquement l'adresse de l'expéditeur dans la liste de blocage si l'e-mail soumis est un spam ou un hameçon. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.

Tableau 3-4 Paramètres de soumission à Secure Content Management

Paramètre et valeur par défaut		Description
SCMENABLED	0 (Non)	Active la soumission des échantillons à une solution SCM. 0 = non. 1 = oui. Toute autre valeur est considérée comme étant égale à 0.
SCMRELAYSERVER « mail.exemple.com »		Le nom ou l'adresse IP du serveur SMTP (par exemple, serveur1.domaine1 ou 192.168.255.200).
SCMRELAYPORT	25	Port du serveur SMTP. Son numéro est compris entre 1 et 65535.
SCMSPAMADRESS « échantillon_spam@exemple.com »		Adresse e-mail de soumission des spams ou hameçons ignorés.
SCMHAMADRESS « échantillon_non-spam@exemple.com »		Adresse e-mail de soumission des non-spams ou non-hameçons.

Exemples

Mettez les chaînes de caractères entre guillemets. Par exemple :

```
INSTALLDIR1="C:\FOLDER A\FOLDER 1"
```

La commande ci-dessous installe silencieusement Customer Submission Tool en utilisant les valeurs par défaut. Dans la barre d'outils Microsoft Outlook, seuls les boutons **Soumettre des spams ou hameçons** et **Soumettre des non-spams ou non-hameçons** s'affichent. A la fin de l'opération, aucun redémarrage ne se produit. Dans ce type d'installation, l'utilisateur ne soumet des échantillons qu'aux laboratoires McAfee. Il ne peut pas reconfigurer l'outil.

```
msiexec /qn /i mcst.msi CONFIGENABLED=0 INSTALLDIR1="C:\FOLDER A\FOLDER 1" REBOOT=R
```

La commande ci-dessous installe silencieusement Customer Submission Tool. Elle permet non seulement de soumettre des échantillons à McAfee Quarantine Manager, mais aussi de reconfigurer l'outil.

```
msiexec /qn /I mcst.msi MQMENABLED=1 MQMPATH="http://mqm1/userui" REBOOT=R
```

La commande ci-dessous installe Customer Submission Tool. Elle permet de soumettre des échantillons à une solution Secure Content Management. Lors de l'installation, l'utilisateur visualise l'avancement de l'opération. Il peut reconfigurer l'outil.

```
msiexec /i mcst.msi SCMENABLED=1 SCMRELAYSERVER="http://server1" SCMRELAYPORT=1234
```

Annonce d'installation aux utilisateurs e-mail

Vous pouvez annoncer aux utilisateurs e-mail l'installation de Customer Submission Tool dans leur client de messagerie Microsoft Outlook.

Exemple

Actuellement, nous déployons McAfee Customer Submission Tool.

Cet outil nous aidera à réduire le nombre de SPAMS reçus dans l'entreprise. Intégré à Microsoft Outlook, il sera utilisable à l'aide de deux boutons supplémentaires. Si ces options présentées ci-dessous ne s'affichent pas, redémarrez le client de messagerie.

Cliquez sur ce bouton pour soumettre des spams ignorés :

Cliquez sur ce bouton pour soumettre des e-mails identifiés à tort comme étant des spams :

Modification de la configuration

Pour modifier la configuration sans avoir à réinstaller l'outil, vous pouvez changer les paramètres de la clé de registre suivante :

HKEY_CURRENT_USER\Software\McAfee\Submission Tool

Les paramètres sont répertoriés dans le tableau suivant.

Tableau 3-5 Valeurs de registre par défaut

Nom	Valeur par défaut (en hexadécimal)
AseEnabled	00000001
AseResponseFreq	00000000
AseResponseType	00000000
BlacklistSpamOnSubmit	00000000
ConfigEnabled	00000001
DeleteSpamOnSubmit	00000000
DontShowHamSubmit	00000000
DontShowSpamSubmit	00000000
MaxSubmissionCount	00002710
MqmEnabled	00000000
MqmPath	« http://mqm.exemple.com/mqmuserui »
ScmDataTimeout	0000ea60
ScmEnabled	00000000
ScmHamAddress	« échantillon_non-spam@exemple.com »
ScmRecvTimeout	0000ea60
ScmRelayPort	00000019
ScmRelayServer	« mail.exemple.com »
ScmSendTimeout	0000ea60
ScmSpamAddress	« échantillon_spam@exemple.com »
WhitelistHamOnSubmit	00000000

Les noms du registre sont identiques à ceux des paramètres de la section *Installation de l'outil à l'aide d'un script, page 19*.

Certains, non disponibles en tant que paramètres, sont définissables uniquement depuis le registre. Par exemple, les valeurs de temporisation SCM entrent dans ce cadre. Elles sont par défaut égales à 60 000 millisecondes (1 minute).

Pour appliquer les paramètres de registre modifiés, redémarrez Microsoft Outlook. Si vous saisissez des valeurs incorrectes, l'outil les remplace par les éléments par défaut.

4 Utilisation du logiciel

Boutons et entrées de menus

Une fois installé, Customer Submission Tool ajoute une barre d'outils et des entrées de menus (reportez-vous à la figure 2-1, page 14) au client Microsoft Outlook, pour permettre de :

- Soumettre des e-mails qui auraient dû être considérés comme des spams ou des hameçons.
  Reportez-vous aux sections *Soumission de votre premier échantillon de spam ou d'hameçon* et *Soumission d'autres échantillons de spams ou d'hameçons, page 25*.
- Soumettre des e-mails qui ont été classés par erreur dans la catégorie des spams ou des hameçons.
  Reportez-vous aux sections *Soumission de votre premier échantillon classé dans la mauvaise catégorie, page 25* et *Soumission d'autres échantillons classés dans la mauvaise catégorie, page 26*.
- Ajouter tous vos contacts Microsoft Outlook à une liste d'autorisation (si McAfee Quarantine Manager est activé). Reportez-vous à la section *Ajout de vos contacts Microsoft Outlook à la liste d'autorisation, page 27*.
- Configurer certains paramètres du logiciel. Reportez-vous à la section *Configuration du logiciel, page 27*.

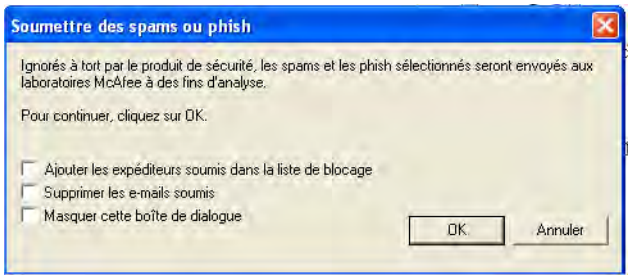
Soumission de votre premier échantillon de spam ou d'hameçon

Lorsque vous soumettez un échantillon pour la première fois, vous pouvez configurer le logiciel à votre convenance. Pour soumettre un échantillon de spam ou d'hameçon, procédez comme suit :

1 Dans Microsoft Outlook, affichez le message ou sélectionnez l'objet du message.

2 Dans la barre d'outils, cliquez sur le bouton **Soumettre des spams ou hameçons**. Vous pouvez aussi utiliser le menu **Actions**. Une boîte de dialogue s'ouvre :

Figure 4-1 Boîte de dialogue d'envoi d'échantillons



3 Sélectionnez les fonctions de votre choix :

Fonction	Description
Ajouter les expéditeurs soumis dans la liste de blocage	Cette case n'est disponible que si McAfee Quarantine Manager est en cours d'exécution. Cette option ajoute l'expéditeur du spam à une liste de blocage. Les prochains e-mails qu'il enverra seront bloqués.
Supprimer les e-mails soumis	Cette option supprime tous les échantillons de spams ou d'hameçons sélectionnés, après leur soumission.
Masquer cette boîte de dialogue	Empêche cette boîte de dialogue d'apparaître à nouveau. Pour que cette boîte de dialogue s'affiche à nouveau à l'avenir, cliquez sur le bouton **Soumettre des spams ou hameçons** tout en maintenant la touche MAJ enfoncée.

Cliquez sur **OK** pour fermer la boîte de dialogue. Vous venez d'envoyer l'échantillon.

4 Si vous soumettez l'échantillon à McAfee Quarantine Manager, vous êtes invité à entrer votre nom de connexion et votre mot de passe.

5 Un message apparaît pour vous indiquer que l'échantillon a bien été envoyé. Cliquez sur **OK**.

Le logiciel ne peut pas soumettre d'échantillons trop volumineux (plus de 1 Mo). McAfee vous recommande donc de supprimer ces fichiers.

Soumission d'autres échantillons de spams ou d'hameçons

Pour soumettre un échantillon de spam ou d'hameçon, procédez comme suit :

1 Dans Microsoft Outlook, affichez le message ou sélectionnez l'objet du message.

Il est possible de soumettre plusieurs échantillons à la fois à partir de la liste des objets d'e-mails. Pour sélectionner plusieurs e-mails à soumettre en une seule fois, utilisez la touche MAJ. Pour sélectionner plusieurs e-mails qui ne se suivent pas dans la liste, utilisez la touche CTRL.

2 Dans la barre d'outils, cliquez sur le bouton **Soumettre des spams ou hameçons**. Vous pouvez aussi utiliser le menu **Actions**.

Si une boîte de dialogue apparaît, sélectionnez les fonctions de votre choix. Reportez-vous à la section *Soumission de votre premier échantillon de spam ou d'hameçon, page 24*. Si aucune boîte de dialogue ne s'affiche, cliquez en maintenant la touche MAJ enfoncée pour l'afficher. Cliquez sur **OK** pour fermer la boîte de dialogue.

Vous venez d'envoyer l'échantillon.

3 Un message apparaît pour vous indiquer que l'échantillon a bien été envoyé. Cliquez sur **OK**.

Le logiciel ne peut pas soumettre d'échantillons trop volumineux (plus de 1MO). McAfee vous recommande donc de supprimer ces fichiers.

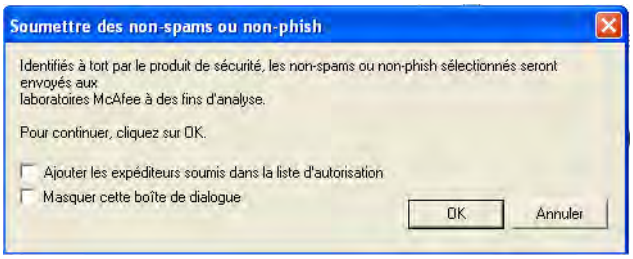
Soumission de votre premier échantillon classé dans la mauvaise catégorie

Lorsque vous soumettez un échantillon pour la première fois, vous pouvez configurer le logiciel à votre convenance. Pour soumettre un échantillon qui a été classé par erreur dans la catégorie des spams ou des hameçons :

1 Dans Microsoft Outlook, affichez le message ou sélectionnez l'objet du message.

2 Dans la barre d'outils, cliquez sur le bouton **Soumettre un échantillon de non-spam**. Vous pouvez aussi utiliser le menu **Actions**. Une boîte de dialogue s'ouvre :

Figure 4-2 Boîte de dialogue d'envoi d'échantillons



3 Sélectionnez les fonctions de votre choix :

Fonction	Description
Ajouter les expéditeurs soumis dans la liste d'autorisation	Cette case n'est disponible que si McAfee Quarantine Manager est en cours d'exécution. Les prochains e-mails envoyés par cet expéditeur ne seront pas considérés comme des spams.
Masquer cette boîte de dialogue	Pour que cette boîte de dialogue s'affiche à l'avenir, vous pouvez cliquer sur le bouton **Soumettre un échantillon de non-spam** tout en maintenant la touche MAJ enfoncée.

4 Cliquez sur **OK** pour fermer la boîte de dialogue. Vous venez d'envoyer l'échantillon.

5 Si vous soumettez l'échantillon à McAfee Quarantine Manager, vous êtes invité à entrer votre nom de connexion et votre mot de passe.

6 Un message apparaît pour vous indiquer que l'échantillon a bien été envoyé. Cliquez sur **OK**.

Le logiciel ne peut pas soumettre d'échantillons trop volumineux (plus de 1MO). McAfee vous recommande donc de supprimer ces fichiers.

Soumission d'autres échantillons classés dans la mauvaise catégorie

Pour soumettre un échantillon qui a été classé par erreur dans la catégorie des spams ou des hameçons :

1 Dans Microsoft Outlook, affichez le message ou sélectionnez l'objet du message.

Il est possible de soumettre plusieurs échantillons à la fois à partir de la liste des objets d'e-mails. Pour sélectionner plusieurs e-mails à soumettre en une seule fois, utilisez la touche MAJ. Pour sélectionner plusieurs e-mails qui ne se suivent pas dans la liste, utilisez la touche CTRL.

2 Dans la barre d'outils, cliquez sur le bouton **Soumettre un échantillon de non-spam**. Vous pouvez aussi utiliser le menu **Actions**.

Si une boîte de dialogue apparaît, sélectionnez les fonctions de votre choix (tel que décrit à la section *Soumission de votre premier échantillon classé dans la mauvaise catégorie, page 25*), puis cliquez sur **OK** pour fermer la boîte de dialogue. Si aucune boîte de dialogue ne s'affiche, cliquez en maintenant la touche MAJ enfoncée pour l'afficher. Cliquez sur **OK** pour fermer la boîte de dialogue.

Vous venez d'envoyer l'échantillon.

3 Un message apparaît pour vous indiquer que l'échantillon a bien été envoyé. Cliquez sur **OK**.

Le logiciel ne peut pas soumettre d'échantillons trop volumineux (plus de 1MO). McAfee vous recommande donc de supprimer ces fichiers.

Ajout de vos contacts Microsoft Outlook à la liste d'autorisation

Cette fonction n'est disponible que si McAfee Quarantine Manager est installé et si Customer Submission Tool est configuré de manière à afficher le bouton **Configurer les paramètres de soumission** dans la barre d'outils.

Pour éviter que les e-mails provenant de vos contacts Microsoft Outlook soient considérés comme des spams (ou des hameçons), vous pouvez ajouter les adresses de vos contacts à votre liste d'autorisation :

1. Dans Microsoft Outlook, cliquez sur le bouton **Configurer les paramètres de soumission** de la barre d'outils.
2. Dans la boîte de dialogue **Customer Submission Tool**, cliquez sur **Ajouter des contacts à la liste d'autorisation**.
3. Cliquez sur **OK** pour fermer la boîte de dialogue.

Dorénavant, les e-mails qui vous seront envoyés par des contacts figurant dans votre liste d'autorisation ne seront pas analysés pour rechercher d'éventuels spams ou hameçons. La recherche de virus est toujours effectuée sur tous les e-mails.

Configuration du logiciel

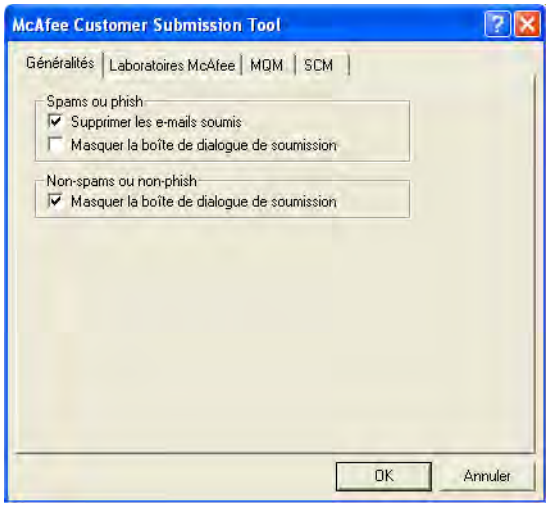
Si le bouton **Configurer les paramètres de soumission** est disponible dans la barre d'outils, vous pouvez configurer certaines fonctions de Customer Submission Tool. Ce bouton n'est disponible que lors de l'affichage des objets d'e-mails.

Il n'est pas disponible si le logiciel a été installé via un script qui ne l'a pas activé.

Pour configurer le logiciel :

1. Cliquez sur le bouton **Configurer les paramètres de soumission** de la barre d'outils pour ouvrir une boîte de dialogue :

Figure 4-3 Boîte de dialogue de configuration



2 Sélectionnez les fonctions de votre choix :

Intitulé	Description de la fonction
Supprimer les e-mails soumis	Cette option supprime tous les spams et hameçons après leur soumission effective.
Masquer la boîte de dialogue de soumission	Cette option empêche toute boîte de dialogue d'apparaître lorsqu'un spam ou un hameçon (ou un e-mail considéré comme tel) est soumis au laboratoire.

3 Si vous avez l'intention de soumettre des échantillons aux laboratoires de McAfee pour analyse, sélectionnez l'onglet **Laboratoires McAfee**, cliquez sur **Activer**, puis sélectionnez une autre valeur :

Intitulé	Description de la fonction
Fréquence de réponse	Indique la fréquence à laquelle les laboratoires McAfee doivent vous envoyer un e-mail automatiquement pour accuser réception de vos soumissions. Si vous avez sélectionné l'option **Immédiatement** et si vous envoyez plusieurs échantillons en même temps, vous risquez de recevoir plusieurs réponses dans les minutes qui suivent.
Type de réponse	Indique le niveau de détail pour chaque e-mail automatique. Par exemple, **Résumé** correspond à un simple accusé de réception.

Lorsque vous utilisez le logiciel pour la première fois, McAfee vous recommande de sélectionner les options **Immédiatement** et **Résumé**.

4 Si vous avez l'intention de soumettre des échantillons à McAfee Quarantine Manager, sélectionnez l'onglet **MQM**, cliquez sur **Activer**, puis sélectionnez les options suivantes :

Intitulé	Description de la fonction
URL	Adresse du serveur MQM, du type : ■ http://www.exemple.com ■ 192.168.255.200
Nom d'utilisateur	Nom d'utilisateur (ex. utilisateur@exemple.com) utilisé pour les communications directes avec MQM.
Mot de passe	Mot de passe associé au nom d'utilisateur.
Ajouter l'adresse soumise des expéditeurs dans la liste de blocage	Les prochains e-mails qu'il enverra seront bloqués.
Ajouter l'adresse soumise des expéditeurs dans la liste d'autorisation	Aucune recherche de spams ou d'hameçons ne sera effectuée sur les prochains e-mails envoyés par cet expéditeur. Seule la recherche de virus sera effectuée.

5 Si vous avez l'intention de soumettre des e-mails à Secure Content Management, sélectionnez l'onglet **SCM**, cliquez sur **Activer**, puis sélectionnez les options suivantes :

Intitulé	Description de la fonction
Serveur	Nom du serveur, du type : ■ serveur1 ■ 192.168.255.200 ■ mailto:192.168.255.200 ■ http://exemple.com/utilisateur ■ http://exemple.com/utilisateur:8080/utilisateur1/dossier1
Port	Numéro de port, par exemple 25.
Spams ou hameçons	Adresse (celle configurée sur la solution), telle que spam@exemple.com.
Non-spams ou non-hameçons	Adresse (celle configurée sur la solution), telle que non-spam@exemple.com.

6 Cliquez sur **OK** pour fermer la boîte de dialogue. Les nouveaux paramètres sont pris en compte tout de suite.