Guide de l'utilisateur final

Websense TRITON AP-EMAIL Cloud

10240 Sorrento Valley Rd., San Diego, CA 92121, États-Unis

Publié le août 5, 2015
Imprimé aux États-Unis d'Amérique et en Chine.

Marques déposées

Sommaire

1 Utilisation de TRITON AP-EMAIL

Introduction

Bienvenue dans le *Guide de l'utilisateur de TRITON AP-EMAIL*. Votre organisation s'est abonnée au service TRITON AP-EMAIL fourni par Websense.

Ce guide décrit le fonctionnement du service et vous explique comment prendre le contrôle de votre messagerie électronique et comment réduire le nombre de courriers indésirables, également appelés pollupostage.

Qu'est-ce que Websense TRITON AP-EMAIL ?

Websense TRITON AP-EMAIL est un service qui filtre tous les messages entrants et sortants en provenance d'Internet (c'est-à-dire hors du domaine interne de votre entreprise). Il analyse les messages entrants avant qu'ils n'atteignent votre réseau et filtre les messages non désirés selon la stratégie définie par votre administrateur de messagerie.

TRITON AP-EMAIL est généralement utilisé pour filtrer les messages contenant des virus ou du pollupostage, bien qu'il soit également capable de bloquer d'autres types de contenu, tels que les messages accompagnés de fichiers vidéo ou exécutables et les messages contenant des mots ou des phrases inappropriés.

Comment ce logiciel va-t-il affecter mon travail ?

La plupart du temps, vous n'aurez pas conscience du fonctionnement de Websense TRITON AP-EMAIL. Vous recevrez votre courrier normalement, mais vous remarquerez peut-être une diminution du volume de courriers indésirables.

TRITON AP-EMAIL peut communiquer avec vous de deux manières :

1. **Notification de courrier électronique** : Vous serez parfois averti(e) qu'un message a été bloqué. Ceci se produira uniquement lorsqu'une personne a tenté de vous envoyer un message électronique contenant un virus ou tout autre type de contenu non autorisé. La notification peut contenir un lien sur lequel vous pourrez cliquer pour obtenir plus d'informations sur le message bloqué.
2. **Rapport sur les messages destiné à l'utilisateur final :** TRITON AP-EMAIL peut vous envoyer régulièrement un rapport de messages. Ce rapport vous renseigne sur tous les courriers électroniques que vous avez reçus et envoyés et vous permet de décider quoi faire avec les messages considérés comme du pollupostage. Pour plus d'informations, consultez *Comment saurai-je quels messages ont été bloqués ?*, page 3.

TRITON AP-EMAIL va-t-il affecter les personnes qui m'envoient du courrier électronique ?

Non. Le service n'avertit pas les expéditeurs lorsque leur message contient un virus et a été bloqué.

Comment TRITON AP-EMAIL gère-t-il le pollupostage ?

Tous les messages filtrés par TRITON AP-EMAIL sont analysés et un score de pollupostage leur ait attribué. Plus ce score est élevé, plus le message est susceptible d'être du pollupostage. Votre entreprise a défini un seuil et tous les messages qui le dépasse seront classés en tant que pollupostage.

Dans ce cas, les messages sont généralement mis en quarantaine et conservés pendant 30 jours. Les messages dont le score de pollupostage est élevé peuvent être détruits sous le contrôle de l'administrateur. Vous ne serez **PAS** averti(e) lorsque vous recevez du pollupostage. Dans certaines organisations, 98 pourcent du courrier entrant est du pollupostage. Vous n'aimeriez pas être averti(e) à chaque message indésirable reçu.

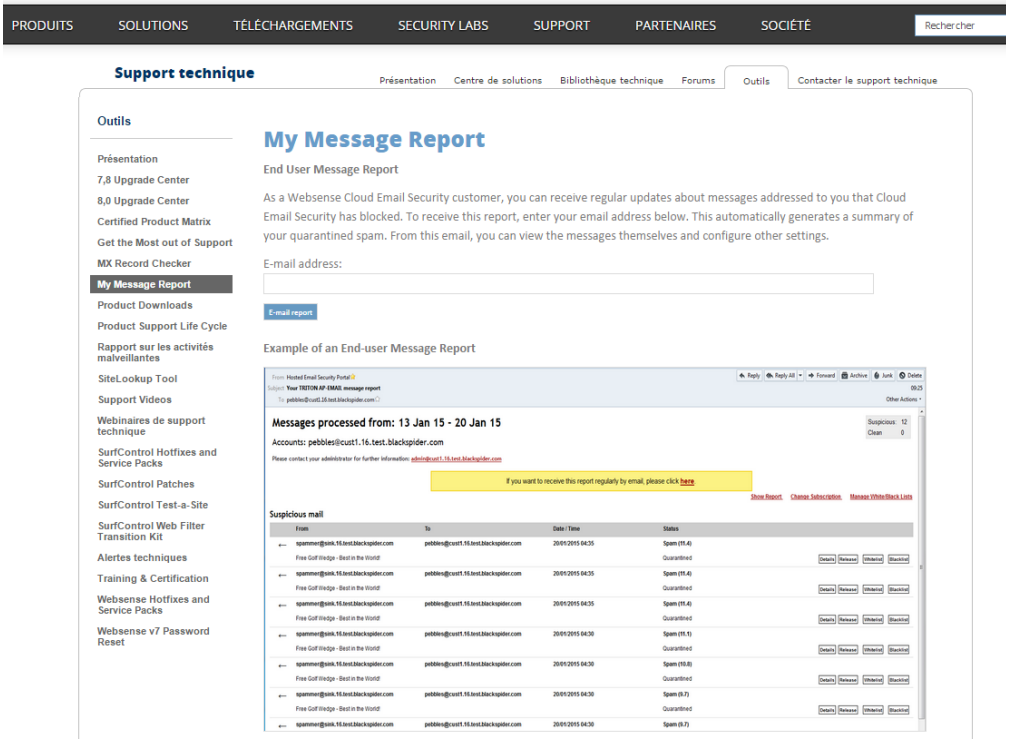
Le service TRITON AP-EMAIL peut marquer un courrier comme étant du pollupostage. Dans ce cas, il est livré normalement, mais le mot « Pollupostage » est ajouté à l'objet. Cette fonctionnalité est le plus souvent configurée par l'administrateur de messagerie pour la période d'essai initiale ou pour étiqueter les messages dont le score de pollupostage est dans la limite du supportable.

Comment saurai-je quels messages ont été bloqués ?

TRITON AP-EMAIL peut vous fournir un rapport qui énumère tous les messages traités pour votre adresse électronique, y compris ceux qui ont été bloqués.

Pour obtenir ce rapport, visitez la page Web suivante :

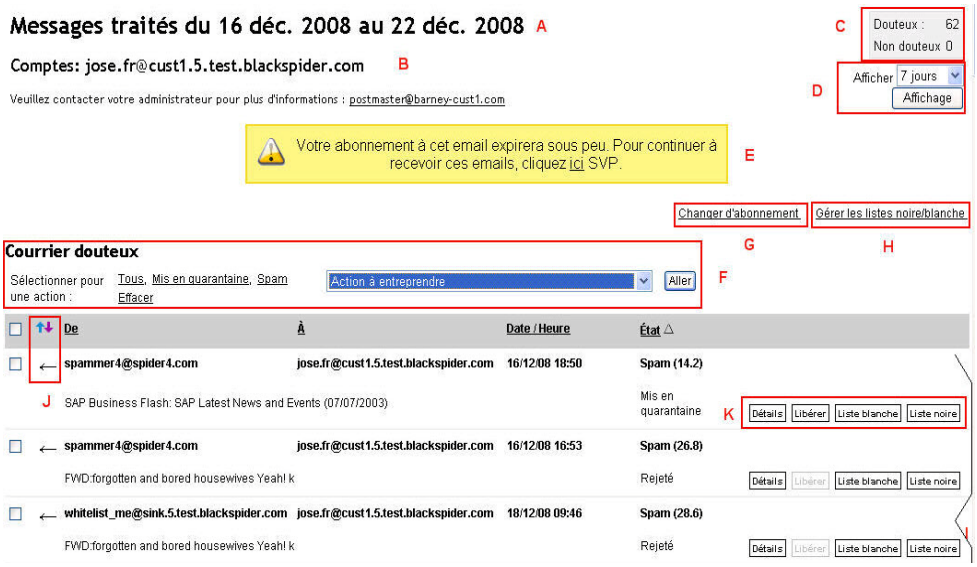
http://www.websense.com/content/messagereport.aspx



Entrez votre adresse électronique dans le champ fourni, et vous recevrez le rapport. Cela ne prend que quelques minutes, selon la quantité de données.

Que comprend le rapport de messages ?

Ce rapport comprend de nombreuses informations utiles. L'exemple suivant montre la version en ligne du rapport, à laquelle vous pouvez accéder en cliquant sur **Afficher les rapports**.



	Contenu
A	Plage de dates du traitement du rapport
B	Votre adresse électronique
C	Nombre de messages suspects et légitimes qui ont été traités pendant cette période
D	Option qui permet de modifier le nombre de jours affichés dans le rapport
E	Lien pour recevoir régulièrement ce rapport par courrier électronique
F	Possibilité de sélectionner tous les messages en quarantaine ou de pollupostage et de leur appliquer une action, telle que supprimer ou libérer
G	Lien pour modifier votre abonnement au rapport
H	Lien pour gérer vos propres listes noires et blanches
I	Liste de vos messages triés dans l'ordre suivant (selon la configuration de votre compte et de vos paramètres d'utilisateur) : • Messages suspects reçus ou envoyés • Messages légitimes reçus ou envoyés Si vous observez la version en ligne de votre rapport, vous remarquerez que vous pouvez modifier l'ordre des messages en cliquant sur le lien de l'en-tête des colonnes. Par exemple, vous pouvez les trier selon les critères suivants : colonne **De** ou **À**, **Date/Heure** ou **État**.

	Contenu
J	Indication précisant si un message a été reçu ou envoyé. ← Reçu → Envoyé
K	Actions que vous pouvez entreprendre pour un message. (Sélectionnez un message en cochant la case à sa gauche.) Options proposées : • **Détails** - Accédez aux détails du message. • **Libérer** - Sortez le message de sa quarantaine. (Pas possible pour tous les messages, notamment ceux contenant des virus connus) • **Liste blanche** - Ajoutez cette adresse électronique ou ce domaine à votre propre liste blanche. Ainsi, les messages de cet expéditeur ou de ce domaine seront toujours autorisés, à moins qu'ils ne contiennent un virus ou un programme malveillant. • **Liste noire** - Ajoutez cette adresse électronique ou ce domaine à votre propre liste noire. Ainsi, les messages de cet expéditeur ou de ce domaine ne seront jamais autorisés.

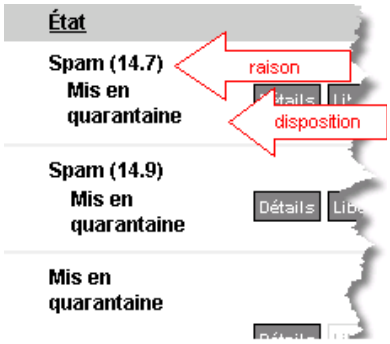
Informations de la section Résumé d'un message :

- Le message est entrant ou sortant.
- L'expéditeur du message
- Le destinataire du message
- L'heure et la date à laquelle le service TRITON AP-EMAIL a enregistré le message
- L'état du message. Cela comprend une raison et une disposition. (Pour plus d'informations, consultez *Que signifie l'État ?*, page 6.)
- L'objet du message

Que signifie l'État ?

La colonne **État** du rapport comprend une raison, telle que Spam pour du pollupostage, et une disposition, telle que Mis en quarantaine.

Si un message n'a pas été livré, le premier mot (en gras) de cette colonne indique pourquoi. Le mot suivant indique l'action entreprise, également appelée disposition.



Les messages mis en quarantaine comprennent leur score de pollupostage. Plus ce score est élevé, plus le message est susceptible d'être du pollupostage.

Le tableau suivant décrit les raisons que vous pouvez rencontrer :

Raison	Explication
Contrôle d'accès	Le message a été bloqué à cause d'une règle de contrôle d'accès définie par votre administrateur.
Règle d'accès	Le message a été bloqué à cause d'une règle de contrôle d'accès définie par votre administrateur.
Pièce jointe bloquée	Le message contenait une pièce jointe dont le type a été bloqué par votre stratégie.
Fichier exécutable bloqué	Le message contenait une pièce jointe exécutable et ce type de fichier est bloqué par votre stratégie.
Élément de la liste noire	L'adresse électronique ou le domaine de cet expéditeur figure dans votre liste noire ou dans celle de votre stratégie.
Non douteux	Le message ne viole aucune disposition de votre stratégie.

Raison	Explication
Contenu dangereux	Le contenu du message peut être dangereux pour votre ordinateur. Cette raison peut comporter des raisons sous-jacentes : **Double extension** - Le nom de fichier d'une pièce jointe possède une double extension, ce qui peut masquer la fonction réelle du fichier. **Archive vide** - Le message contient un fichier d'archive vide. **Exécutable dans un message de service** - Le message est un message d'état de livraison qui comporte du contenu exécutable. **openrelay(block)** - L'expéditeur du message n'aurait pas dû être autorisé à envoyer du courrier via ce serveur de messagerie. **Virus par usurpation** - Le message contient un virus. L'expéditeur du message semble falsifié. **Pièces jointes suspectes** - ThreatSeeker a détecté une pièce jointe suspecte $1 dans le message. **Archive zéro octet** - Le message contient une pièce jointe d'archive vide. Un virus en a probablement été retiré. **Exécutable zéro octet** - Le message contient une pièce jointe exécutable vide. Un virus en a probablement été retiré.
Extension masquée	Le message contient une pièce jointe dont l'extension a été renommée selon la configuration de votre stratégie. Par exemple, une extension exécutable peut avoir été nommée .ex_ pour éviter son exécution.

Raison	Explication
Format	Cette raison peut comporter des raisons sous-jacentes : • **Échec de l'extraction de l'archive** - Le service n'a pas réussi à décompresser et à analyser un fichier d'archive. • **Nom de fichier de pièce jointe manquant** - La pièce jointe au message n'a pas de nom de fichier spécifié. Cette pratique peut servir à exploiter certains clients de messagerie. • **Email non composite** - La structure du message est potentiellement malveillante et peut servir à attaquer certains clients de messagerie. • **Crypté** - Le message ou une pièce jointe est crypté(e). • **Niveau d'expansion dépassé** - Le message contient trop de niveaux d'archives imbriqués. Le contenu de l'archive ne peut pas être analysé. • **Nom de fichier bloqué** - Le nom d'une pièce jointe correspond à une règle configurée de service. • **Nom de fichier trop long** - L'objet contient un nom de fichier trop long. Cette pratique peut servir à attaquer certains clients de messagerie. • **En-tête bloqué** - L'en-tête du message viole une règle de stratégie en vigueur. • **Bloc d'en-tête trop long** - L'en-tête du message contient un bloc de données plus volumineux que le maximum autorisé. • **En-tête trop long** - L'en-tête du message dépasse la longueur autorisée. Cette pratique peut servir à attaquer certains clients de messagerie. • **Objet bloqué** - L'objet du message correspond à une règle configurée de service. • **Type MIME bloqué** - Le message contient une pièce jointe qui est bloquée par la stratégie en vigueur. • **Message incomplet** - Le message ne peut pas être analysé car des parties sont manquantes dans la pièce jointe. Il a été bloqué. • **Archive protégée par mot de passe** - Le message contient un fichier d'archive protégé par un mot de passe. Il ne peut pas être analysé et a donc été bloqué. • **Exploit Outlook potentiel** - La date ou l'objet du message est trop long(ue). Cette pratique peut servir à attaquer certains clients de messagerie, tels que les anciennes versions de MS Outlook. • **Signé** - Le message a été signé cryptographiquement. Il ne peut pas être analysé et a donc été mis en quarantaine. • **Caractères suspects** - Le corps du message contient des informations binaires imprévues. Cette pratique peut être malveillante. • **Caractères d'en-tête suspects** - L'en-tête du message contient des informations binaires imprévues. Cette pratique peut être malveillante. • **Destinataire non routable** - La stratégie de messagerie bloque l'envoi des messages vers ce sous-domaine. • **Expéditeur non routable** - La stratégie de messagerie bloque l'envoi des messages provenant des utilisateurs de ce sous-domaine.

Raison	Explication
Liste grise	Le message semble suspect. Nous le conservons pour procéder à une investigation plus approfondie.
Règle lexicale	Le contenu du message viole une règle lexicale en vigueur dans votre stratégie.
Macro	Le message est suspecté de contenir un virus de type macro.
Boucle de message	Le service a détecté une boucle de livraison de message.
Opérationnel	Le message a été bloqué pour des raisons opérationnelles.
Virus potentiel	Le message contient un virus potentiel susceptible d'endommager votre ordinateur.
Spam (n)	Le message a été classifié comme pollupostage par votre stratégie de messagerie. Les messages mis en quarantaine comprennent leur score de pollupostage. Plus ce score est élevé, plus le message est susceptible d'être du pollupostage.
Système	Le traitement du message a échoué pour des raisons système.
Échec temporaire	Le serveur de messagerie est interrompu temporairement et dans l'incapacité de recevoir les messages.
Trop volumineux	Le message est plus volumineux que la taille autorisée par la stratégie en vigueur.
Inconnu	Le message a rencontré un problème inconnu.
Virus	Le message contient un virus connu susceptible d'endommager votre ordinateur.
Élément de la liste blanche	L'adresse électronique ou le domaine de cet expéditeur figure dans votre liste blanche ou dans celle de votre stratégie.

Le tableau suivant énumère les dispositions possibles :

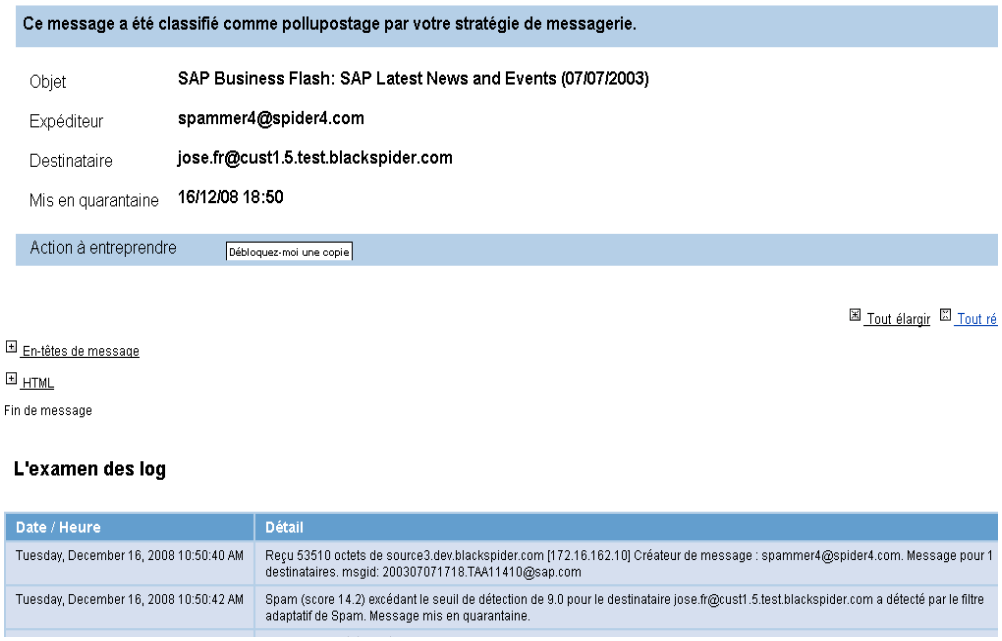
Disposition	Explication
Accepter	Le message a été accepté et livré.
Bcc	Une copie cachée du message a été envoyée (le nom du destinataire était masqué).
Bcc, objet marqué	Une copie cachée du message a été envoyée avec la ligne de l'objet marquée.
Renvoyé	Ne pouvant pas être livré, le message a été renvoyé à l'expéditeur.
Contournement	Le message a contourné le système de sécurité de la messagerie.
Abandonné	Le message a été supprimé des archives.
Mis en quarantaine	Le message est conservé en quarantaine.
Spam transmis	Ce message de pollupostage a été transmis à un destinataire.
Objet marqué	L'objet du message a été marqué.
Échec temporaire	Le serveur de messagerie est interrompu temporairement et dans l'incapacité de recevoir les messages.

Disposition	Explication
Inconnu	L'action résultante est inconnue.
Néant	Aucune action n'a été entreprise.

Si vous avez besoin d'un message qui a été bloqué ou placé en quarantaine à cause des paramètres de votre stratégie, veuillez contacter votre administrateur de messagerie.

Comment puis-je accéder à mes courriers électroniques ?

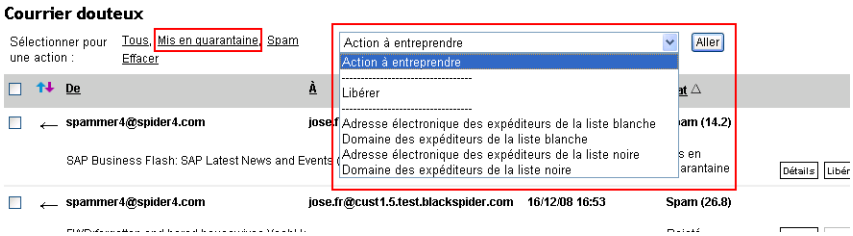
Dans votre rapport de messages, vous pouvez voir d'un coup d'œil tous les messages qui vous ont été envoyés de l'extérieur du réseau, y compris ceux qui ont été classifiés comme pollupostage et ceux qui ont été placés en quarantaine pour d'autres raisons. Pour voir le contenu d'un message, sélectionnez-le (en cochant la case à sa gauche), puis cliquez sur **Détails**. Vous obtenez alors ceci :



Dans cet exemple, un message a été mis en quarantaine car la stratégie l'a classé en tant que pollupostage. L'administrateur vous autorise à en recevoir une copie. Si ces fonctions n'étaient pas activées par l'administrateur, les boutons n'apparaitraient pas à l'écran. Dans certains cas, vous serez autorisé(e) à ajouter un message aux listes noire ou blanche ou encore à libérer le message. Toutefois, si le message a été mis en quarantaine car il contient un virus ou des mots inappropriés, vous ne serez pas autorisé(e) à en libérer une copie, quelle que soit la manière dont l'administrateur a configuré le service.

Pour gérer tous vos messages placés en quarantaine en une seule opération, cliquez sur **Mis en quarantaine** sous **Choisir une action** dans votre rapport, puis choisissez

l'action désirée. Vous pouvez libérer des éléments de la quarantaine et mettre les adresses ou les domaines dont ils proviennent en liste blanche ou noire.



Vous pouvez exécuter des actions sur certains messages en cochant leurs cases individuelles, puis en choisissant un bouton tel que **Liste blanche** ou **Liste noire**.

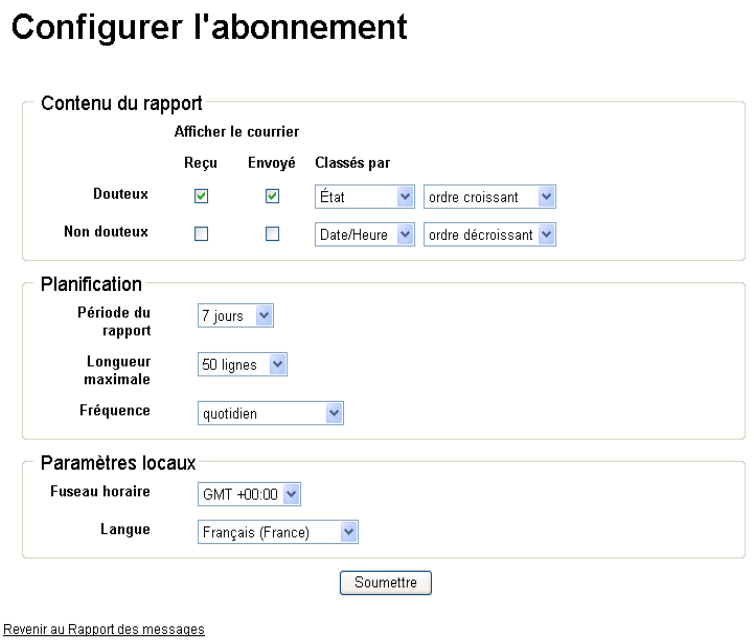
TRITON AP-EMAIL conserve-t-il une copie de mes courriers électroniques ?

Par défaut, TRITON AP-EMAIL ne conserve pas de copies des messages, à moins qu'ils ne soient mis en quarantaine, bien que votre administrateur puisse configurer votre système différemment. Les messages en quarantaine sont automatiquement supprimés après 30 jours, ou votre administrateur peut les supprimer chaque fois que nécessaire.

Si vous cliquez sur un lien du rapport des messages pour effacer un message, seules les entrées du journal de messagerie apparaissent car ce message n'est plus disponible pour TRITON AP-EMAIL.

TRITON AP-EMAIL peut-il m'envoyer automatiquement le rapport des messages ?

Vous pouvez configurer TRITON AP-EMAIL pour qu'il vous envoie ces rapports à l'intervalle de votre choix. Pour définir les détails de l'abonnement, demandez un rapport, puis, dans celui-ci, cliquez sur le lien **Changer l'abonnement.** Vous obtenez alors un écran ressemblant à celui-ci.



Vous pouvez choisir les options d'abonnement suivantes :

- Contenu du rapport
  - Quelles sections voulez-vous inclure dans le rapport : messages douteux reçus ou envoyés, messages non douteux reçus ou envoyés ?
  - Dans quel ordre les informations doivent-elles apparaître : date/heure, objet, de, à, état ? Ordre croissant ou décroissant ?
- Planification
  - Quelle durée le rapport doit-il couvrir : les derniers 1, 2, 7, 14 ou 30 jours ?
  - Combien de lignes doivent apparaître dans le rapport : 20, 50, 100, 200 ou 500 ?
  - Quelle doit être la fréquence de livraison du rapport : quotidienne, jours de la semaine, hebdomadaire, bihebdomadaire, mensuelle ou jamais ?

Remarque

Les abonnements au rapport de messages du service TRITON AP-EMAIL sont périmés après 90 jours. 62 jours après votre abonnement, à chaque réception du rapport, le système vous rappelle de renouveler votre abonnement.

- Localisation
  - Quel fuseau horaire votre rapport doit-il utiliser ?
  - Dans quelle langue voulez-vous recevoir le rapport ? TRITON AP-EMAIL prend en charge 14 langues :
    - Tchèque
    - Hollandais
    - Anglais
    - Français
    - Allemand
    - Grec
    - Italien
    - Polonais
    - Portugais (Brésilien)
    - Portugais
    - Roumain
    - Slovaque
    - Espagnol
    - Suédois

Comment puis-je annuler mon abonnement aux rapports ?

Vous pouvez annuler cet abonnement à tout moment. Dans l'un des rapports, cliquez sur le lien **Changer l'abonnement**. Dans l'écran de configuration de l'abonnement, sélectionnez **jamais** dans la zone déroulante **Fréquence** sous **Planification**, puis cliquez sur **Appliquer**.

Quels que soient les paramètres du rapport planifié, vous pouvez également demander un rapport imprévu en remplissant le formulaire que vous trouverez à cette adresse http://www.websense.com/content/messagereport.aspx.

Puis-je changer les paramètres dans mes rapports de message ?

Vous pouvez changer les détails de cet abonnement à tout moment. Dans l'un des rapports, cliquez sur le lien **Changer l'abonnement**. Dans l'écran de configuration de l'abonnement, modifiez les options selon vos désirs.

Comment TRITON AP-EMAIL détecte-t-il le pollupostage ?

TRITON AP-EMAIL utilise un moteur de détection très perfectionné qui est constamment mis à jour pour identifier les nouveaux types de pollupostage. Le pollupostage évoluant continuellement, TRITON AP-EMAIL utilise un moteur

adaptatif capable de tirer des enseignements des expériences précédentes et des commentaires des utilisateurs. Nous employons également des analystes du pollupostage pour examiner les messages ambigus et mettre à jour le moteur de détection si nécessaire.

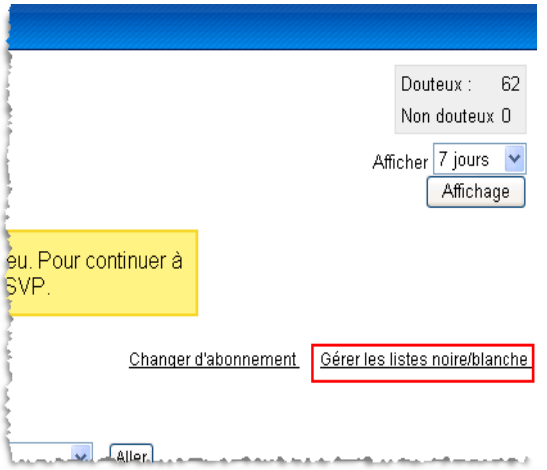
Comment empêcher TRITON AP-EMAIL de bloquer les messages que je souhaite recevoir ?

La définition de pollupostage est subjective ; ce qui est du spam pour un utilisateur ne l'est pas pour un autre. C'est la raison pour laquelle TRITON AP-EMAIL risque parfois de bloquer un message que vous souhaitez recevoir. C'est particulièrement le cas avec les newsletters et les messages en volume qui possèdent des caractéristiques de pollupostage.

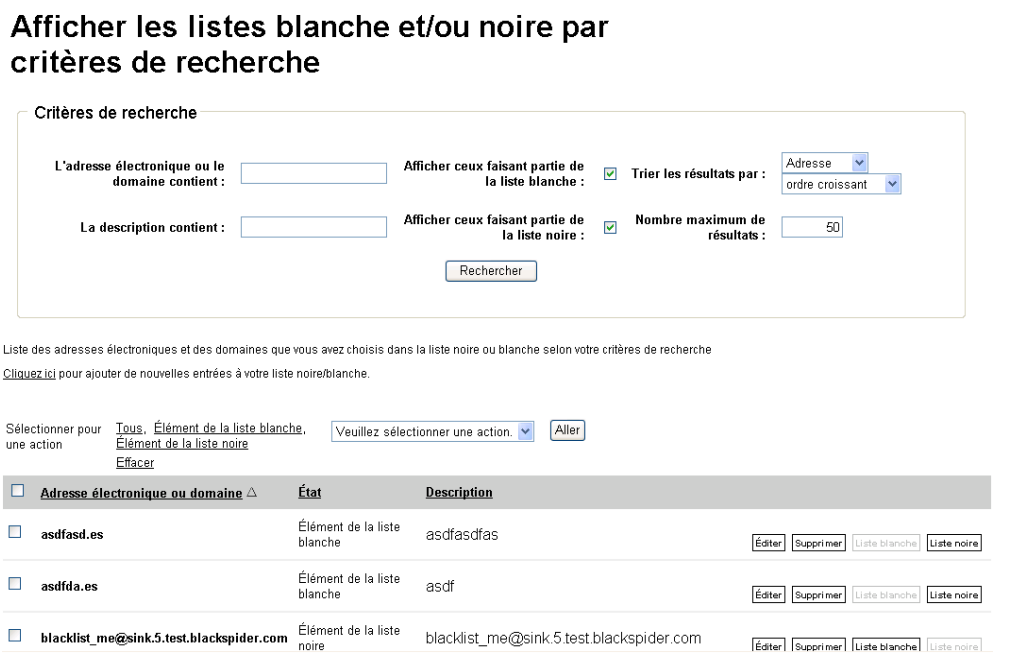
Pour empêcher TRITON AP-EMAIL de bloquer ces messages à l'avenir, ajoutez leurs expéditeurs à votre liste blanche (si votre administrateur vous a accordé cette option). Les messages provenant d'une personne qui figure dans votre liste blanche ne sont jamais classifiés comme pollupostage. Pour ajouter un expéditeur à votre liste blanche, localisez son message dans le rapport, sélectionnez-le en cochant sa case, puis cliquez sur le bouton **Liste blanche**.

Dans l'écran suivant, utilisez la liste déroulante pour choisir une action : **Adresse électronique des expéditeurs de la liste blanche** ou **Domaine des expéditeurs de la liste blanche**, puis cliquez sur **Aller**.

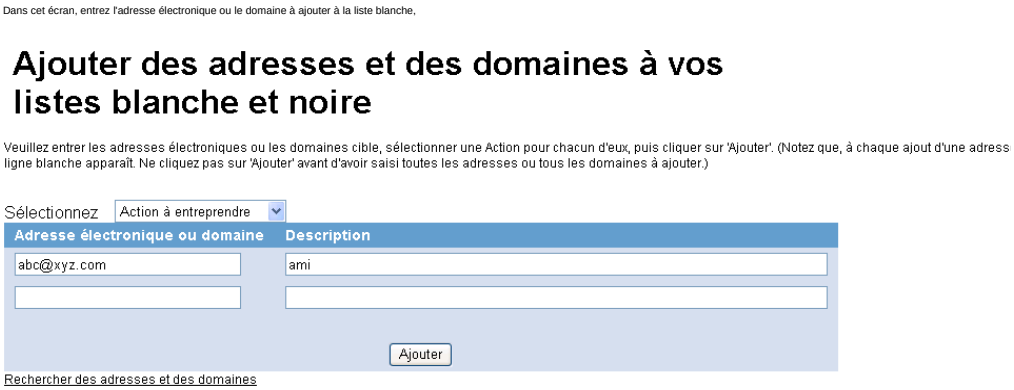
Pour afficher ou gérer toute votre liste blanche, sélectionnez **Gérer les listes noire/ blanche** dans votre rapport.



Dans l'écran suivant, vous pouvez rechercher les adresses électroniques ou les domaines de votre liste blanche. Cliquez sur **Afficher ceux faisant partie de la liste blanche**, entrez des critères de recherche, tels que l'adresse à localiser, puis cliquez sur **Rechercher**. Vous pouvez choisir l'ordre de tri des résultats, ainsi que le nombre de résultats.



Si une adresse n'apparaît pas dans votre liste blanche mais que vous souhaitez l'y mettre, cliquez sur le lien Cliquez ici **pour ajouter de nouvelles entrées à votre liste noire/blanche.**



Dans cet écran, entrez l'adresse électronique ou le domaine à ajouter à la liste blanche, puis choisissez **Liste blanche** dans la zone déroulante **Action à entreprendre**.

Si le message qui a été bloqué n'était ni une newsletter ni un message en volume et que vous pensez que TRITON AP-EMAIL l'a classifié par erreur, vous pouvez envoyer une copie du message à l'adresse spam@mailcontrol.com. L'équipe d'étude du pollupostage de Websense examine ces messages et, si nécessaire, met le moteur de détection à jour.

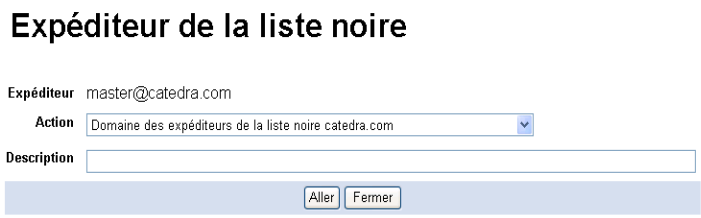
Pourquoi TRITON AP-EMAIL n'a-t-il pas bloqué le pollupostage que j'ai reçu ?

Websense met constamment à jour son moteur de filtrage du pollupostage pour détecter les nouvelles formes de spam. TRITON AP-EMAIL détecte correctement plus de 99 pourcent de tout le pollupostage qui pénètre dans le service. Toutefois, la définition de pollupostage est subjective ; ce qui est du spam pour un utilisateur ne l'est pas pour un autre.

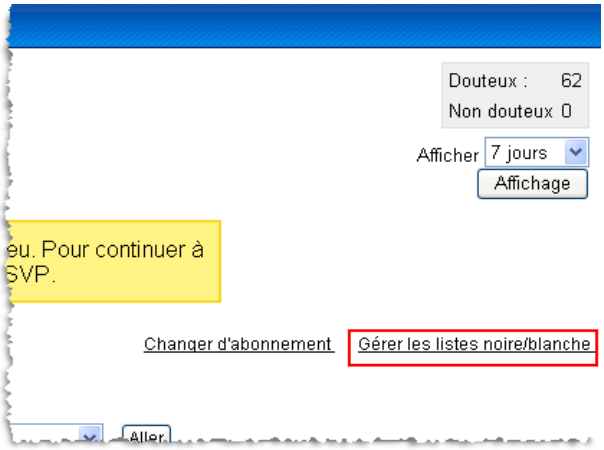
Pour que TRITON AP-EMAIL cesse de vous livrer les messages provenant d'un expéditeur particulier à l'avenir, vous pouvez ajouter ce dernier à votre liste noire (si votre administrateur vous a accordé cette option). Les messages provenant d'une personne qui figure dans votre liste noire sont toujours classifiés comme pollupostage.

Pour ajouter un expéditeur à votre liste noire, localisez son message dans le rapport, sélectionnez-le en cochant sa case, puis cliquez sur le bouton **Liste noire**.

Dans l'écran suivant, utilisez la liste déroulante pour choisir une action : **Adresse électronique des expéditeurs de la liste noire** ou **Domaine des expéditeurs de la liste noire**, puis cliquez sur **Aller**.

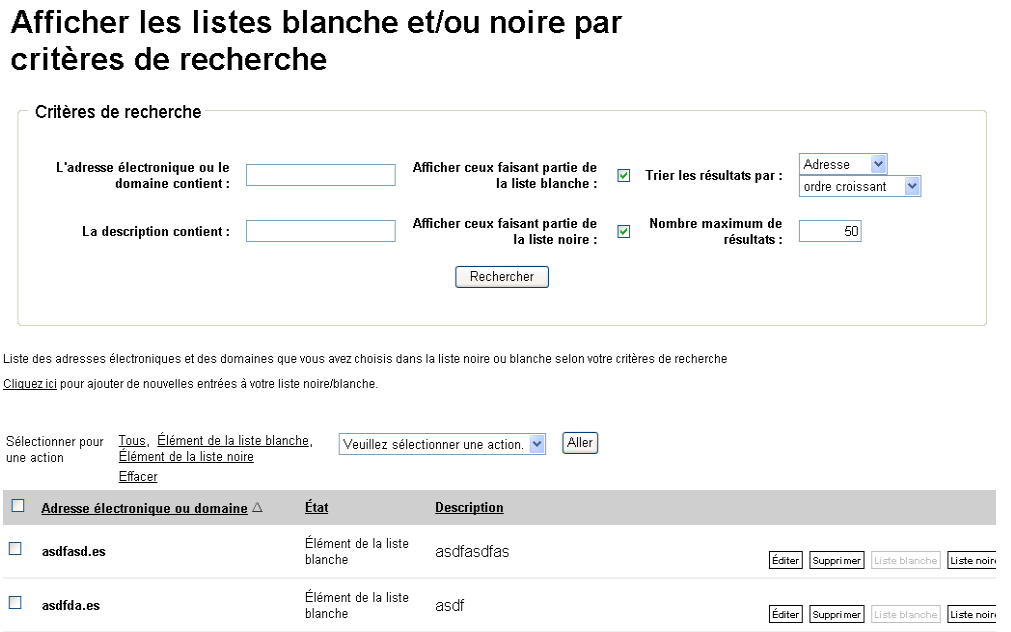


Pour afficher ou gérer toute votre liste noire, sélectionnez **Gérer les listes noire/blanche** dans votre rapport.

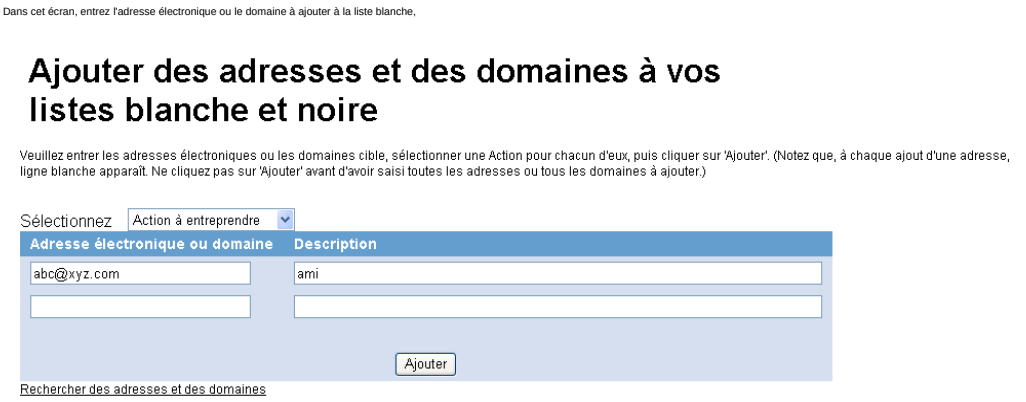


Dans l'écran suivant, vous pouvez rechercher les adresses électroniques ou les domaines de votre liste noire. Cliquez sur **Afficher ceux faisant partie de la liste noire**, entrez des critères de recherche, tels que l'adresse à localiser, puis cliquez sur

Rechercher. Vous pouvez choisir l'ordre de tri des résultats, ainsi que le nombre de résultats.



Si une adresse n'apparaît pas dans votre liste noire mais que vous souhaitez l'y mettre, cliquez sur le lien Cliquez ici **pour ajouter de nouvelles entrées à votre liste noire/ blanche.**



Dans cet écran, entrez l'adresse électronique ou le domaine à ajouter à la liste noire, puis choisissez **Liste noire** dans la zone déroulante **Action à entreprendre**.

Si vous pensez que TRITON AP-EMAIL a classifié un message par erreur, veuillez en informer Websense (si vous en avez la possibilité). Ceci nous permet d'affiner le travail du service TRITON AP-EMAIL. Si votre administrateur a autorisé cette fonction, un lien apparaît en bas de vos messages : « Cliquez ici pour signaler que ce message est du spam ». Lorsque vous cliquez sur ce lien, vous recevrez une confirmation.

Comme nous l'avons déjà expliqué, la définition de pollupostage étant subjective, Websense ne peut pas automatiquement classifier tous les messages similaires à celui-ci comme spam. Vous pouvez nous aider à améliorer notre service. Tous les clients en bénéficieront. Si vous ne souhaitez plus recevoir de messages de cet expéditeur, veuillez l'ajouter à votre liste noire.

Recommandations pour la gestion du pollupostage

Situation	Action à entreprendre
Vous recevez des messages d'une personne et vous souhaitez que cela cesse.	Ajoutez cet expéditeur à votre propre liste noire**.** (Cette fonction doit être activée par votre administrateur.)
Vous recevez un message que vous ne considérez pas comme du pollupostage.	Ajoutez cet expéditeur à votre propre liste blanche**.** (Cette fonction doit être activée par votre administrateur.)
Vous recevez un message à caractère commercial non sollicité.	Cliquez sur le lien « Signaler ce message comme étant du spam » en bas de votre message. L'utilisation de ce service permet d'améliorer la future détection du pollupostage. Pour les messages de texte uniquement où ce lien n'apparaît pas, transmettez-les à spam@mailcontrol.com.
Vous ne souhaitez plus recevoir les newsletters ou la littérature marketing que vous receviez auparavant.	Annulez votre abonnement à cet expéditeur ou placez-le dans votre liste noire. Ne cliquez pas sur le lien « Signaler ce message comme étant du spam », car les autres utilisateurs souhaitent peut-être continuer à recevoir ces messages.
Vous recevez des newsletters ou des offres d'une entreprise avec qui vous étiez en contact, mais vous n'en attendiez aucune communication. (Vous avez peut-être donné par inadvertance votre accord pour être ajouté(e) à leur liste de messagerie.)	