

FAQ Support

Questions récurrentes

Numéro de version	1.0
Auteur	François Brunet
Date de publication	18/09/2018

*L'information contenue dans ce document est sujette à changement périodique. Ce document contient des informations confidentielles.
Tous droits réservés. Aucune partie de ce document ne peut être photocopiée, reproduite, ou traduite dans une autre langue.*

Table des matières

1. Les mails de mes correspondants sont bloqués en SPAM.R	3
2. Je reçois des mails de ma propre adresse alors que je n'ai rien écrit.....	3
3. Je viens de recevoir un virus alors que le mail était filtré par Secuserve.....	4
4. Je n'ai pas reçu mon rapport de quarantaine.	4
5. Je reçois des alertes de boîte over quota, alors que je n'ai pas utilisé tout mon espace autorisé.	5
6. Après avoir configuré ma boîte Secuserve en POP ou en IMAP, je peux recevoir mes mails je n'arrive pas à les envoyer.	5
7. Je rencontre des lenteurs dans l'utilisation de mes boîtes mail.	5
8. Je ne peux pas modifier un rendez-vous que je n'ai pas créé sur un calendrier qu'on m'a partagé et sur lequel j'ai les droits complets.	6
9. J'ai des répertoires sur Pronto où je range mes mails et je ne les vois pas sur mon client de messagerie.	6
10. Je ne vois que quelques mails sur mon téléphone, pourtant j'ai réglé la période de synchro sur 1 mois.	7
11. La taille de mon mail avec sa pièce jointe est largement supérieure à celle du seul fichier joint.....	7
12. Que se passe-t-il au-delà du seuil de destruction des mails ?.....	7
13. J'utilise un téléphone Android, et le corps de mes mails ne s'affiche pas.	7
14. Je constate des dysfonctionnements dans la synchronisation/Partage des calendriers sur mon smartphone.	7
15. Pas de notification (administrateur/émetteur/destinataire) en cas de réception d'un Virus bloqué par le service E-Securemail.	8
16. Communicate a disparu de l'onglet complément de Outlook.	8
17. J'ai besoin de faire faire, par Secuserve, des opérations qui engagent notre responsabilité.	8
18. Je reçois beaucoup de SPAM.....	9
19. Limites d'envoi de messages	9
20. Supprimer les conversations IM et leurs historiques.	9
21. Partager un calendrier avec une personne extérieure.....	9
22. Mes invitations sont automatiquement acceptées ou refusées, et je ne les reçois pas. 10	
23. Champs SPF.....	10
24. Champs MX.....	10
25. Pool IP de Secuserve	11

1. Les mails de mes correspondants sont bloqués en SPAM.R

Lors d'un doute sur un mail reçu (SPF incorrect, IP listée, domaine douteux, etc...) notre infrastructure active l'anti-bombing ou « zone grise » : Le mail est d'abord refusé une première fois (421 throttle: firsttry) en demandant au serveur expéditeur de se représenter plus tard. Une fenêtre de validité temporelle entre 2 minutes et 1h est ensuite ouverte :

- Si le mail se représente **en dessous de 2 minutes**, il sera **refusé (421 throttle early)**
- Si le mail se représente **au-delà d'une heure**, il sera **refusé (421 throttle late)**
- S'il se représente dans la fenêtre de validité, il passe alors dans notre moteur d'analyse antispam

Cette zone grise permet de bloquer efficacement une grande majorité des menaces 0-day, la plupart des serveurs de SPAM ne se représentant jamais ou bien une unique fois et trop vite.

Il est possible de contourner cette mise en zone grise en **whitelisting l'adresse IP du serveur émetteur**. Toutefois tous les envois en provenance de cette adresse ne seront alors plus analysés par l'antispam.

2. Je reçois des mails de ma propre adresse alors que je n'ai rien écrit.

Les mails envoyés avec une adresse mail fausse ne peuvent pas être contrés, n'importe qui peut envoyer un mail avec l'adresse de présentation de son choix (sa propre adresse, noreply@domaine, support@, ou une adresse existante). Il s'agit d'une fonctionnalité du protocole SMTP.

Cette usurpation d'identité n'est toutefois pas complète car l'adresse affichée ne l'est que sur l'en-tête MIME (celle qui apparaît dans votre client de messagerie), et non pas sur l'entête SMTP (celle qui permet la transaction avec le serveur à l'envoi). Pour utiliser une image simple, l'adresse de retour que vous mettez sur une enveloppe postale peut être celle que vous voulez (adresse en Chine par exemple), mais cela ne changera pas la provenance réelle du mail (votre bureau de poste, par exemple)

Ce type de spam, dont les adresses mails de l'expéditeur et du destinataire sont identiques, est populaire car ils peuvent passer les filtres si votre adresse (ou votre domaine) est whitelisted.

Dans le cas où l'adresse SMTP est également usurpée et passe malgré notre filtre anti-bombing décrit plus haut, il peut alors être intéressant d'activer l'anti-spoofing au niveau de la console d'administration. Vous pouvez vous reporter au manuel d'administration de la console ou son aide en ligne pour obtenir plus d'information sur la mise en œuvre de cette option.

3. Je viens de recevoir un virus alors que le mail était filtré par Secuserve.

Le virus en question est passé par notre système de filtrage et n'a pas été détecté au moment de son passage par nos différents moteurs d'antivirus (ESET, DrWeb, ClamAV, etc.) mis à jour toutes les dix minutes.

C'est un cas rare de virus inconnu des services antiviraux internationaux au moment où vous l'avez reçu, certainement car il a tout juste été créé. Vous avez été dans les premiers destinataires de cette attaque virale ce qui est impossible à éviter par les systèmes Anti-Virus (qui fonctionnent par apprentissage), autant en filtrage que localement sur l'ordinateur.

Vous pouvez tester la détection d'une menace par les principaux antivirus du marché en envoyant le fichier ou le lien pour lequel vous avez un doute à VirusTotal :

<https://www.virustotal.com>

Nous vous invitons également à bloquer les fichiers exécutables (.EXE, .js, etc.) dans la console d'administration afin de renforcer la sécurité de vos Boîtes aux Lettres.

4. Je n'ai pas reçu mon rapport de quarantaine.

Le rapport de quarantaine est envoyé chaque jour aux utilisateurs abonnés à leur quarantaine ayant reçu au moins un message mis en quarantaine.

Les messages mis en quarantaine peuvent l'être pour les raisons suivantes :

1. Le **score du message** est compris entre la valeur du seuil de mise en quarantaine et la valeur du seuil de destruction (**Verdict SPAM.A**)
2. Le mail a été détecté comme **PNS** (Pub, News, Social) à condition que la mise en quarantaine de ces classifications soit activée dans la configuration du filtrage (Filtrage > Configuration)
3. Le mail est **trop volumineux**, à condition que la taille limite soit définie dans la configuration du filtrage (**verdict Taille**)
4. Le mail contient **une pièce jointe** répondant aux critères définis dans la configuration du filtrage (**verdict Contenu**)

Les raisons pour lesquelles un utilisateur peut ne pas recevoir son rapport de quarantaine sont les suivantes :

1. **Il n'est pas abonné** à son rapport de quarantaine. Les abonnements doivent en effet être créés via la console dans **Filtrage > Quarantaine > Ajouter un abonnement**. Il peut également s'abonner automatiquement en **envoyant un mail** ayant comme sujet le caractère « * » à quarantaine@security-mail.net
2. **Il n'a pas reçu de message** mis en quarantaine depuis le dernier envoi du rapport de quarantaine.

3. **Le serveur rencontre une anomalie** (pic de charge ou dysfonctionnement) retardant l'envoi des rapports de quarantaine.

Remarque : Il est possible de demander l'envoi du rapport de façon ponctuelle en envoyant un mail ayant comme sujet le caractère « ! » à quarantaine@security-mail.net

5. Je reçois des alertes de boîte over quota, alors que je n'ai pas utilisé tout mon espace autorisé.

Les boîtes mail ont 2 limites de taille existantes :

- La taille globale, que vous pouvez modifier sur votre console d'administration, et pouvant atteindre plusieurs dizaines de giga-octets
- La taille d'un répertoire, qui ne peut excéder 2Go. Ceci est dû au système de fichier sur nos serveurs, et ne peut être modifié que par le support.

Nous avons la possibilité en effet de changer le système de fichier de votre boîte aux lettres, vers une nouvelle technologie qui n'est pas soumise à cette limitation de 2Go par dossier. Nous devons pour cela réaliser une opération de conversion du dossier vers le nouveau format. Comme cela pourrait perturber l'utilisation de la BAL de l'utilisateur, nous avons besoin que toutes les connexions à la boîte aux lettres soient coupées (webmail, client de messagerie, smartphone, etc...). L'opération dure entre 30 minutes et 1h.

Une autre solution simple consiste pour l'utilisateur à procéder à l'archivage de ses courriers, ce qui permet d'éviter d'atteindre ces 2Go et assure la pleine utilisation de nos boîtes et services.

6. Après avoir configuré ma boîte Secuserve en POP ou en IMAP, je peux recevoir mes mails je n'arrive pas à les envoyer.

Certains fournisseurs d'accès, Orange et Free notamment, empêchent l'utilisation de serveurs SMTP autres que les leurs, en bloquant le port 25 de votre connexion internet.

Pour contourner cette limitation vous pouvez configurer le serveur d'envoi en **SSL** sur le **port 465**. Ainsi vous aurez une connexion sécurisée et fiable, malgré les limitations de votre FAI.

7. Je rencontre des lenteurs dans l'utilisation de mes boîtes mail.

Si vous remarquez que vos comptes sont lents à l'utilisation, que ce soit sous Outlook ou Pronto, nous vous invitons à effectuer quelques manipulations afin de mieux cibler la provenance des ralentissements :

- Un traceroute (tracert sous windows) depuis la machine qui subit les lenteurs, vers notre serveur. Ceci pour définir les équipements réseau entre vous et Secuserve, et pointer une défaillance.
- Un ping vers notre serveur, afin de vérifier l'état de la connexion. Faites un ping de 50 sauts (ping -n 50 nomduserveur) pour obtenir un résultat éloquent.

Gardez ces résultats en prenant une capture d'écran, et fournissez-les lors de l'ouverture de votre ticket chez Secuserve. Ces simples tests permettront à tous de gagner du temps en localisant mieux la source du problème.

Dans le cas de délais d'attente lors de l'utilisation d'Outlook, voici quelques préconisations afin de réduire cet effet :

- Contrôlez votre connexion internet et votre bande passante. Le protocole MAPI est sensible aux bandes passantes limitées ce qui augmente de facto le temps de travail de l'application, et renforcera les lenteurs ressenties.
- Ne cliquez pas, et sensibilisez vos utilisateurs à ne pas le faire, sur le bouton d'Outlook "Envoyer/Recevoir". L'utilisation de ce bouton, avec le connecteur MAPI, a pour effet de retélécharger tous les en-têtes de messages et synchroniser tous les dossiers de votre boîte, ce qui est coûteux en temps et en bande passante. Les messages sont reçus et envoyés automatiquement en "push", il n'y a donc pas besoin d'utiliser ce bouton.
- Le connecteur MAPI synchronise, lors du lancement d'Outlook, 2 dossiers : la boîte de réception et les éléments envoyés. Les autres dossiers ne sont vérifiés que lorsque vous y accédez. De sorte que ce sont les 2 dossiers que vous devez archiver (déplacer dans d'autres dossiers, supprimer les mails inutiles/trop vieux) pour ne plus subir de blocage lors du lancement d'Outlook.
- Notre système d'auto-archivage, accessible sur votre console d'administration lorsque vous éditez une boîte aux lettres, permet de ranger, mois après mois, le contenu des dossiers "boîte de réception" et "éléments envoyés" dans un dossier créé automatiquement : Archive > année-mois.

Lorsque vous utilisez le connecteur MAPI et que ce dernier "travaille", Outlook ne permet pas de donner la main à l'utilisateur pour naviguer sur l'outil au même moment ; c'est une limitation du logiciel, mais elle indique que le chargement s'effectue. Vous pouvez malgré tout demander à afficher un message d'attente qui peut être plus parlant pour l'utilisateur en vous rendant dans les paramètres de votre compte MAPI, onglet "Dépannage" et en décochant la case "Ne pas afficher le dialogue processus serveur en cours...".

8. Je ne peux pas modifier un rendez-vous que je n'ai pas créé sur un calendrier qu'on m'a partagé et sur lequel j'ai les droits complets.

Ceci est un fonctionnement normal de notre plateforme. Seule la personne qui a créé le rendez-vous et le propriétaire du calendrier où le rendez-vous a été placé ont les droits de modification.

Pour les autres utilisateurs, ils sont invités à travailler sur leur propre copie de ce rendez-vous dans leur calendrier (personne invitée) pour décliner ou modifier le rendez-vous. Ces transactions se font - c'est une norme - par mail.

9. J'ai des répertoires sur Pronto où je range mes mails et je ne les vois pas sur mon client de messagerie.

Les abonnements IMAP permettant la synchronisation avec les clients de messagerie ne sont pas automatiquement créés en même temps que les nouveaux dossiers.

Il faut donc créer les abonnements via le client de messagerie pour voir apparaître les dossiers.

10. Je ne vois que quelques mails sur mon téléphone, pourtant j'ai réglé la période de synchro sur 1 mois.

L'option pour changer la période de synchronisation, sur Android ou sur iPhone, ne fonctionne pas une fois que le compte est créé, dû à un bug des clients de messagerie sur ces téléphones.

Pour corriger cela, supprimez votre compte, puis recréez-le en le paramétrant normalement jusqu'à la page de configuration de la période de synchro. Précisez alors la période voulue. Enfin, finalisez la création de votre compte. La synchronisation devrait alors correspondre à votre réglage. Tout changement ultérieur de cette période ne peut être fait qu'en supprimant une nouvelle fois le compte.

11. La taille de mon mail avec sa pièce jointe est largement supérieure à celle du seul fichier joint

Lors d'un envoi de fichier attaché à un mail, le standard MIME encode la pièce jointe au format texte en base64 afin de pouvoir l'envoyer via le protocole SMTP. Cet encodage augmente la taille de la pièce jointe d'environ 30%.

Il s'agit donc d'une restriction technique dû au protocole SMTP et non d'une anomalie sur notre infrastructure.

Source : https://en.wikipedia.org/wiki/Email_attachment

12. Que se passe-t-il au-delà du seuil de destruction des mails ?

Un mail qui dépasse le seuil de destruction n'est pas livré, pas présent dans les quarantaines, et n'est pas non plus libérable ou récupérable, il est totalement supprimé de notre système.

Prenez garde à ne pas trop descendre ce seuil car vous pourriez perdre des mails importants de manière irrévocable. Nous préconisons 500, et invitons nos clients à ne passer sous les 400 qu'à leurs risques et périls.

13. J'utilise un téléphone Android, et le corps de mes mails ne s'affiche pas.

Un bug est connu sur certains téléphones Android dans la gestion des comptes Exchange.

Ce dysfonctionnement provient du périphérique, et pas de nos serveurs.

14. Je constate des dysfonctionnements dans la synchronisation/Partage des calendriers sur mon smartphone.

Secuserve ne peut être tenu responsable des dysfonctionnements liés à des applications ou des médias spécifiques (type smartphone ou tablette).

Avant de se lancer dans des investigations plus poussées sur votre matériel, l'OS de ce dernier et le client de messagerie utilisé, nous vous recommandons de :

- 1) Vérifier que la fonction souhaitée (Accès au calendrier, accès à la messagerie, partage de calendriers et autres ressources) fonctionne convenablement sur le Webmail.

- 2) Si tel est le cas, nous vous invitons :
 - a. A mettre à jour votre smartphone avec les dernières versions de l'OS et des logiciels associés à la messagerie
 - b. Détruire votre compte sur votre smartphone, et à le créer à nouveau.

15. Pas de notification (administrateur/émetteur/destinataire) en cas de réception d'un Virus bloqué par le service E-Securemail.

Lorsqu'un virus est détecté par le service E-Securemail, il est systématiquement détruit.

La fonction de notification en temps réel n'est pas disponible pour le scénario Virus afin d'éviter :

1. D'encombrer, voir saturer, la boîte aux lettres du destinataire ou de l'administrateur en cas de bombardement viral
2. D'informer l'émetteur de la véracité et de la bonne réception du virus par le destinataire

Toutefois, de multiples rapports sur la menace virus sont disponibles en ligne ou par mail, à partir de la console d'administration.

16. Communigate a disparu de l'onglet complément de Outlook.

La configuration d'un compte MAPI sur Outlook fait normalement apparaître, dans l'onglet compléments, quelques fonctionnalités supplémentaires comme la configuration du message d'absence ou des règles côté serveur. Si jamais ces compléments venaient à manquer, voici le moyen de les remettre :

- Assurez-vous tout d'abord de bien avoir le connecteur MAPI d'installé sur l'ordinateur, et d'avoir un compte MAPI configuré sur Outlook.
- Rendez-vous dans "fichiers" puis "Options"
- Dans le menu de gauche, allez dans "Compléments", puis cliquez tout en bas sur la case "Atteindre..."
- Ici, cochez "Communigate Pro Extension"
- Sauvegardez en cliquant sur OK, et vérifiez la présence du menu dans votre onglet "Compléments".

17. J'ai besoin de faire faire, par Secuserve, des opérations qui engagent notre responsabilité.

Faites parvenir au support (support@secuserve.com) un mail formé de la façon suivante :

Je soussigné, M/Mme *****, titre *****, agissant au nom de la société *****, dont je suis :

- Le représentant légal
- Mandaté par le représentant légal, Mr/Mme *****, titre *****,
(supprimer la mention inutile)

Demande par la présente aux équipes techniques de la société SECUSERVE sise 74 boulevard du 11 novembre 1918 69100 Villeurbanne (RCS de NANTERRE N° 448 971 531

00059), d'effectuer sur la messagerie de l'entreprise *****, qu'elles gèrent, **les opérations** suivantes :

- *Détails des opérations*

Ou

- Toute opération technique, réalisable conformément au contrat de service et faisant l'objet d'un ticket, sur le serveur de messagerie, les Boîtes Aux lettres, les serveurs de stockage et partage de fichiers, les règles de filtrage et de relaying, afférents aux domaines et collaborateurs de la société *. (supprimer la mention inutile)

J'atteste que la société SECUSERVE m'a informé, qu'en effectuant ces opérations, des risques légaux pouvaient engager ma responsabilité civile, pénale et administrative, ainsi que celle de la société *.

Je décharge formellement ce jour la société SECUSERVE de sa responsabilité légale éventuelle sur l'application de **ces opérations**, et m'engage à ne pas la poursuivre pour ces faits, dont j'assume l'entière responsabilité légale et pénale.

18. Je reçois beaucoup de SPAM.

Notre système anti-spam est en constante évolution pour s'adapter aux différentes techniques d'attaque des spammeurs.

N'hésitez pas à nous faire parvenir les attaques SPAM dont vous êtes victimes via le support ou via le lien/bandeau de feedback situé en bas du mail incriminé.

19. Limites d'envoi de messages

Si vous utilisez notre service de relaying (smtp.security-mail.net), vous serez autorisé à envoyer jusqu'à 300 mails par jour et par utilisateur. Au-delà de cette limite, vos envois vous seront retournés par des messages de service (erreur 4xx). Nous pourrions également, en cas d'abus (ou de compromission de compte), bloquer l'envoi de mails pour un utilisateur.

Pour les utilisateurs du service de messagerie, la limite est de 50 destinataires par email et 1000 mails par jour et par utilisateur. Au-delà de cette limite, les messages seront délivrés à vitesse réduite et le compte pourra être bloqué en cas d'abus ou de compromission.

20. Supprimer les conversations IM et leurs historiques.

Il est possible de supprimer les historiques de conversation en vous connectant à votre boîte par le webmail Pronto.

Connectez-vous à votre boîte, puis rendez-vous dans « Chats », et vous trouverez un fichier de log par conversation, que vous pouvez supprimer ou garder à votre convenance.

21. Partager un calendrier avec une personne extérieure.

Vous avez la possibilité de générer une URL vers votre calendrier en .ics, interprétable par tous les clients de messagerie, que vous pourrez partager à quiconque sous ce format :

<http://mails.optimails.com/~utilisateur@domaine.com/pubcal/Calendrier.ics>

Pour ce faire, rendez-vous sur votre boîte aux lettres par le biais du webmail Pronto, puis cliquez sur les paramètres de votre calendrier et activez "Accès public par le web. Vous verrez alors s'afficher l'adresse à fournir à vos collaborateurs extérieurs.

22. Mes invitations sont automatiquement acceptées ou refusées, et je ne les reçois pas.

Cette action automatique est générée par une option qui permet de transformer la boîte mail d'une personne en une boîte mail de ressource (salle de réunion, véhicule, etc..). Celle-ci va donc automatiquement répondre aux invitations en fonction de sa disponibilité dans la tranche horaire demandée.

Pour résoudre le problème, il vous faudra aller sur votre console d'administration, puis dans « Gestion des boîtes aux lettres ». Trouvez alors la ligne correspondante à la boîte aux lettres en question, puis cliquez sur le bouton « modifier ». Enfin, dans la section « Ressource » cochez la case « désactivé ».

23. Champs SPF

Cette technique vise à réduire les possibilités d'usurpation en publiant, dans le DNS, un enregistrement (de type TXT) indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré.

Si vous utilisez nos serveurs pour envoyer du courrier, via notre service de relaying ou nos serveurs de messagerie, vous devez configurer votre domaine pour indiquer nos informations SPF :

IN TXT "v=spf1 include:includespf.security-mail.net -all"

24. Champs MX

Les champs MX d'un domaine permettent d'indiquer vers quel(s) serveur(s) la livraison des messages adressés au domaine doit s'effectuer.

Pour profiter de nos services, les MX de votre domaine doivent être configurés de la façon suivante :

IN MX 10 france.security-mail.net.

IN MX 20 europe.security-mail.net.

Aucun autre champ MX ne doit être renseigné au risque de voir certains mails ne pas passer par notre filtrage.

Le serveur de destination des mails filtrés (votre serveur de messagerie si vous êtes en filtrage) doit également être renseigné au niveau de la console d'administration dans **Administration > Livraison/SMTP > Serveur de destination.**

25. Pool IP de Secuserve

Dans certains cas, vous pouvez avoir besoin de whitelister nos IP ou de n'autoriser les messages qu'en provenance de notre infrastructure (pour empêcher les livraisons en direct – qui ne passent pas par les champs MX mais directement par l'adresse de votre serveur de messagerie). Vous avez alors besoin de savoir avec quelle(s) adresse(s) IP nous pouvons contacter vos serveurs.

Notre **pool IP de sortie** est le suivant : **85.31.212.0/24**

26. Service de relaying SMTP

Pour nos clients utilisant le filtrage, nous proposons un service de relaying de messagerie permettant de profiter des avantages de la Communication avancée (signatures centralisées UniSign) et du suivi des messages envoyés.

Ce service est accessible via l'adresse SMTP : **smtp.security-mail.net** sur les ports **25** ou, dans le cas d'un blocage par votre FAI, **2525**