Avira Managed Email Security (AMES)

Manuel pour les utilisateurs

AVIRA

Table des matières

1. Informations produit

Merci de consulter le Manuel pour les Avira Managed Email Security (AMES).

Ce manuel vous aidera à vous familiariser avec AMES et à personnaliser AMES en fonction de vos besoins. Vous apporterez la paix dans votre boîte de réception en un rien de temps.

1.1 Fonctionnalité

Avira Managed Email Security (AMES) est un service qui arrête les spams ou virus avant qu'ils n'atteignent le réseau de votre entreprise, en acheminant les emails vers notre cluster de serveurs AMES. AMES scanne et délivre les emails exempts de logiciels malveillants à votre serveur.

La technologie d'analyse de spams la plus précise

Pour intercepter les spams, nous utilisons une combinaison de technologies très efficace. Les spammeurs et créateurs de virus devenant plus créatifs tous les jours, nous testons et implémentons constamment de nouvelles méthodes pour conserver notre leadership dans l'analyse d'emails, et vous en bénéficiez sans effort supplémentaire.

Configuration d'AMES

Comme nous stoppons les spams et virus « dans le nuage », c'est aussi là que la configuration est effectuée.

Vous pouvez vous connecter à l'interface AMES à l'adresse https://ames.avira.com.

Actuellement, l'interface AMES est disponible dans les langues suivantes :

- Anglais
- Allemand
- Français
- Espagnol
- Néerlandais

AMES sauvegarde votre choix de langue dans un cookie ou tente de faire correspondre la langue à celle de votre navigateur. Si la langue n'est pas prise en charge, l'interface AMES s'ouvre en anglais.

Notes de mise à jour

Pour que vous soyez au courant des derniers développements, nous avons placé un lien vers la page des **Notes de mise à jour** (disponible uniquement aux niveaux partenaire et administrateur de domaine).

1.2 Octroi de licences AMES

Lorsque vous laissez votre partenaire Avira acheter une licence pour AMES, vous devez choisir le nombre d'utilisateurs. Ces utilisateurs correspondent au nombre total de personnes dans votre organisation qui vont utiliser AMES pour filtrer les emails.

AMES vous confère une liberté totale dans la répartition de ces utilisateurs à travers des domaines multiples, la création d'alias pour eux, la définition de règles de filtrage, etc. mais vous devez toujours maintenir votre licence à jour avec les utilisateurs. Pour de plus amples informations, voir les conditions AMES sur notre site web.

2. Se familiariser avec AMES

Vous allez constater qu'une fois que votre partenaire Avira aura installé une licence pour votre domaine, le reste de la configuration est étonnamment facile.

Si vous n'avez pas encore de partenaire Avira, consultez l'outil Trouver un partenaire sur notre site web.

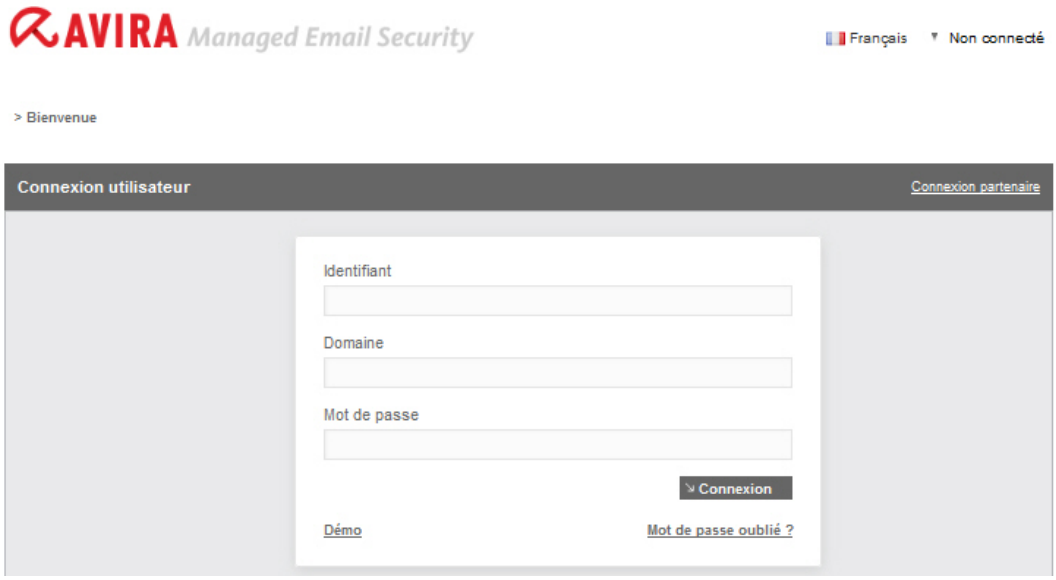
2.1 Ajout d'un nouveau domaine à AMES

Pour ajouter un nouveau domaine à AMES, contactez votre partenaire Avira. Il enregistrera vos coordonnées, demandera une licence et ajoutera le domaine à AMES.

2.2 Connexion à AMES

Le domaine est créé dans AMES et vous recevez un **email de confirmation de commande** avec les données de connexion pour le compte AMES et les détails tels que **Réglages DNS MX** et **Réglages du pare-feu**.

1. Ouvrez https://ames.avira.com dans votre navigateur, où vous trouverez l'écran de connexion :



2. Indiquez votre **Identifiant**, le **Domaine** auquel vous souhaitez accéder et votre **Mot de passe**.

   Ils apparaissent dans la **confirmation de commande** reçue par votre partenaire.

3. Cliquez sur **Connexion**.

Vous verrez s'afficher l'**Accord de licence de service** (SLA) AMES que vous devez lire et accepter pour continuer.

2.3 Configuration du domaine AMES

Pour chaque nouveau domaine, un utilisateur générique est créé (voir « Le catch-all alias » - page 12) et **la livraison des mails** est définie sur le **serveur mail actuellement utilisé**. Cela signifie que vous pouvez commencer à utiliser AMES sans autre configuration et que le flux d'emails ne sera pas interrompu.

Normalement, votre partenaire effectue la configuration du domaine pour vous, mais si vous devez vous en charger, nous vous guiderons à travers ce processus.

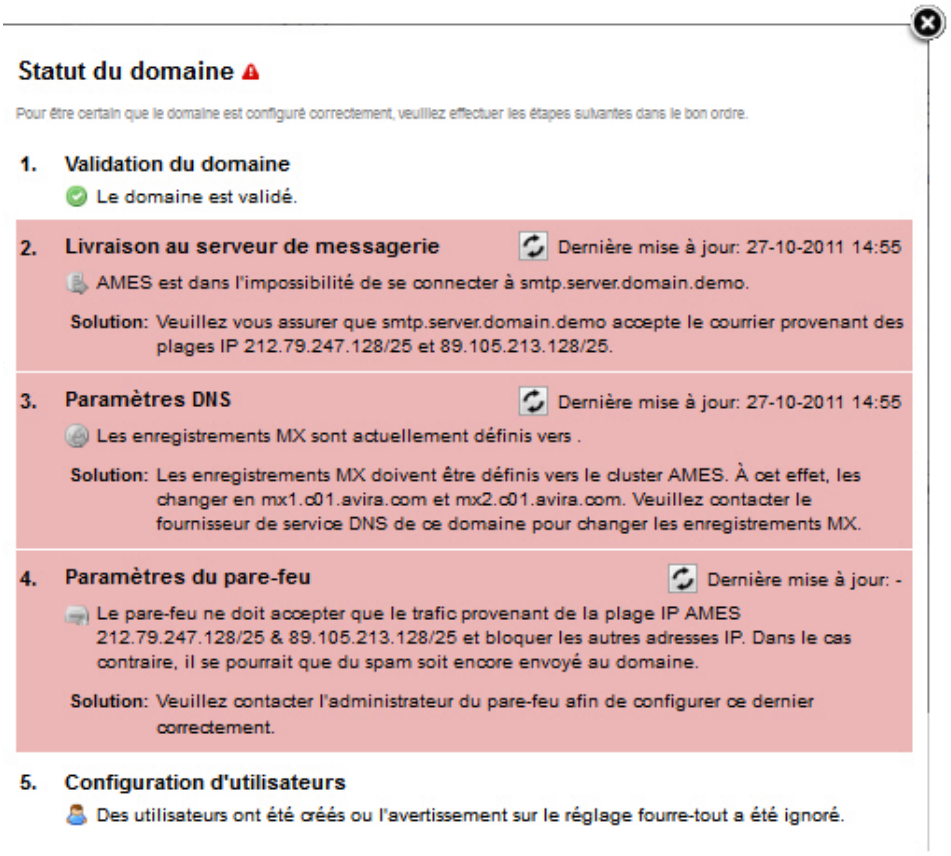
L'assistant Statut du domaine

Une fois connecté à AMES, cliquez sur l'onglet **Services** dans **Aperçu du domaine**.

Le lien **Statut du domaine** ouvre l'assistant d'activation du domaine en 5 étapes qui affiche l'état de chaque étape et affiche finalement des instructions pour les effectuer :

1. Validation du domaine
2. Livraison au serveur de messagerie
3. Paramètres DNS

4. Paramètres du pare-feu
5. Configuration d'utilisateur



Configuration du serveur DNS

Pour activer l'analyse et le filtrage des emails entrants, vous devez changer les **Réglages MX** dans le serveur DNS pour le domaine. Les bonnes données se trouvent dans l'**email de confirmation de commande**.

Si elles sont correctes, les données MX s'affichent en vert sous **Informations sur le DNS du domaine** dans l'onglet **Services** de l'**Aperçu du domaine**.Si les données MX sont incorrectes, un message s'affiche en rouge. Par exemple :

Remarque
Assurez-vous qu'aucune donnée MX n'a une priorité inférieure à 10 ; sinon, les emails de votre organisation ne sont pas analysés ni filtrés par AMES.

En fonction des réglages Time-To-Live (TTL) de vos données MX, l'activation de vos modifications DNS peut prendre jusqu'à 24 heures.

Après avoir dirigé les données MX vers le cluster AMES d'Avira, le service géré est actif et analyse et filtre les emails entrants. Les emails filtrés et analysés seront livrés à la boîte de réception habituelle.

Configuration de la sécurité et du pare-feu

Une fois les modifications DNS terminées et propagées correctement, assurez-vous que le serveur mail de réception n'accepte que les emails en provenance du cluster de serveurs AMES mentionné dans l'**email de confirmation de commande**. Ceci est réalisable via des réglages du pare-feu ou du serveur mail lui-même.

2.4 Analyse des emails sortants

Par défaut, AMES ne scanne que les emails entrants. Le service relais (analyse des emails sortants) est initialement désactivé.

Si vous souhaitez qu'AMES analyse vos emails sortants à la recherche de virus, contactez votre partenaire Avira pour activer la fonction relais pour votre domaine.

Avec le service relais activé, les administrateurs du domaine voient la quantité de messages sortants filtrés.

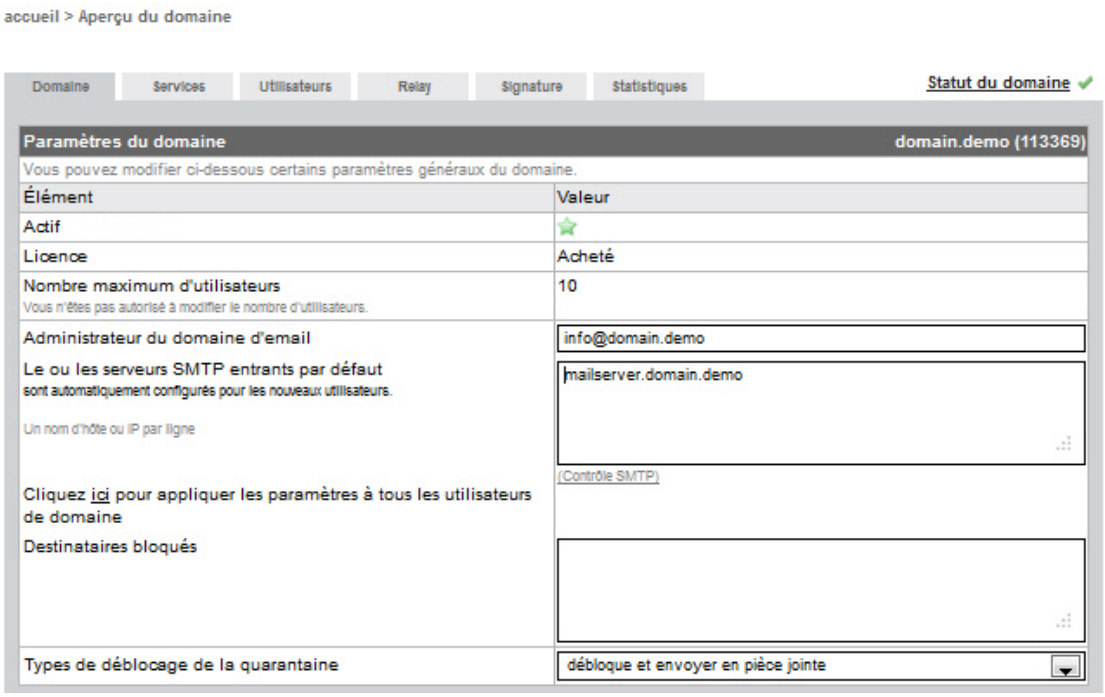
Une quantité journalière maximale de messages est définie en fonction du nombre d'utilisateurs : la quantité d'utilisateurs dans le domaine multipliée par 50 (jamais moins de 1000 messages). Si cette limite est atteinte, les administrateurs reçoivent un message retourné.

3. Configuration de vos domaines et utilisateurs AMES

3.1 Définition des paramètres généraux du domaine

Vérifiez d'abord les paramètres généraux du nouveau domaine.

1. Dans **Aperçu du domaine**, cliquez sur l'onglet **Domaine**.



   Le lien **Statut du domaine** ouvre l'assistant d'activation en 5 étapes du domaine (voir « L'assistant Statut du domaine » - page 7).

2. Votre partenaire peut activer ou désactiver votre domaine.

   Le type de licence et le nombre maximum d'utilisateurs du domaine s'affichent sous *Paramètres du domaine*.

3. Dans le champ **Administrateur du domaine d'email**, tapez l'adresse email de l'administrateur du domaine.

4. Insérez **Le ou les serveurs SMTP entrants par défaut** qui s'appliqueront aux nouveaux utilisateurs que vous créez.

   Ajoutez une seule adresse IP ou nom d'hôte sur chaque ligne.

   Si vous souhaitez attribuer ces serveurs à tous les utilisateurs du domaine, utilisez le lien « Cliquez ici ».

5. Si vous souhaitez bloquer les comptes d'email de certains utilisateurs, mais conserver leurs quarantaines pendant un moment, ajoutez leurs adresses email au champ **Destinataires bloqués**.

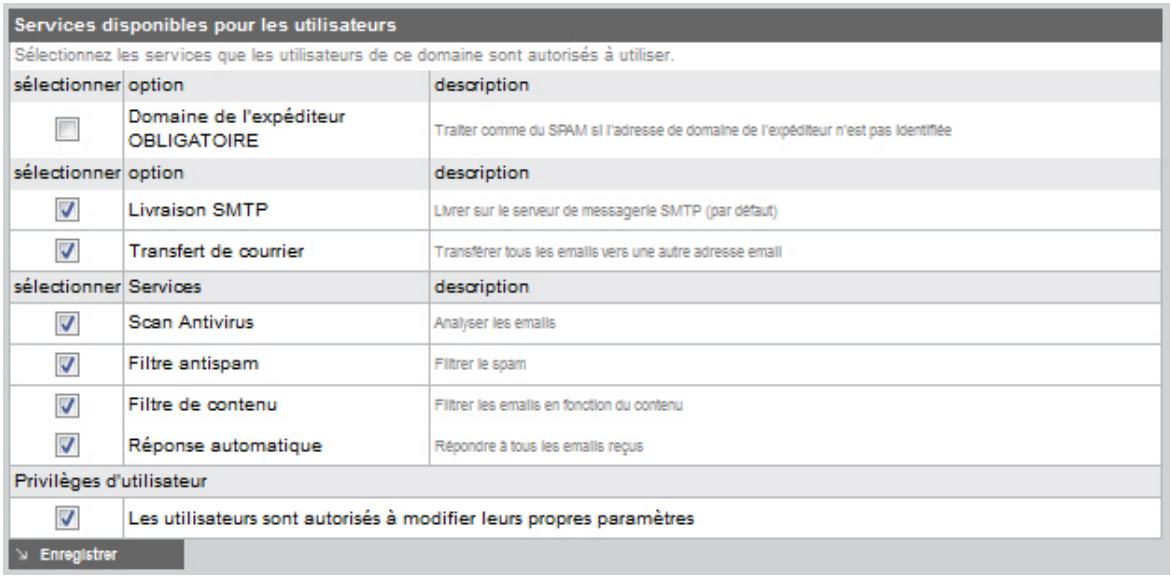
A leur sortie de la quarantaine, les emails bloqués peuvent être livrés comme pièce jointe ou message original. Pour définir ce réglage pour la totalité du domaine, utilisez l'option **Types de déblocage de la quarantaine** :

- **Débloquer et envoyer le message original** - Envoyer le message d'origine dans les boîtes mail des utilisateurs.
- **Débloquer et envoyer en pièce jointe** - Envoyer le message bloqué sous forme de pièce jointe à un email d'avertissement dans les boîtes mail des utilisateurs.

3.2 Configuration des services disponibles pour les utilisateurs finaux

1. Dans **Aperçu du domaine**, cliquez sur l'onglet **Services**.

2. Sous *Services disponibles pour les utilisateurs*, vous pouvez activer ou désactiver certaines options pour tous les utilisateurs finaux du domaine sélectionné.



- **Domaine de l'expéditeur OBLIGATOIRE** - Si le domaine de l'expéditeur n'apparaît pas, le message est considéré comme un spam.
- **Livraison SMTP** - Les messages sont délivrés au serveur mail SMTP.
- **Transfert de courrier** - Les messages sont transférés vers une autre adresse email.
- **Scan Antivirus** - Les messages sont analysés à la recherche de virus.
- **Filtre antispam** - Les messages sont analysés à la recherche de spam.
- **Filtre de contenu** - Les composants du message sont analysés, en fonction des règles de contenus de la liste blanche/liste noire.
- **Réponse automatique** - Les utilisateurs sont autorisés à activer le service de réponse automatique.

- **Les utilisateurs sont autorisés à modifier leurs propres paramètres** - Les utilisateurs peuvent activer les notifications de virus et programmer des rapports de quarantaine.

3.3 Ajout de nouveaux utilisateurs à un domaine

Lorsque AMES est configuré pour votre domaine, les utilisateurs que vous fournissez doivent fonctionner correctement. Si un email est envoyé à l'adresse email `test@demo.domaine`, l'utilisateur `test` doit exister, ou l'email sera retourné à l'expéditeur.

Le catch-all alias

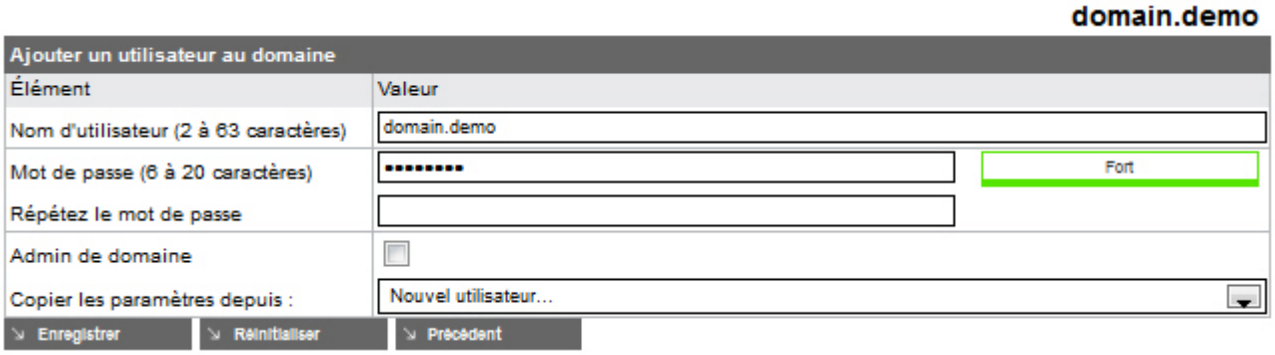
Par défaut, AMES dispose d'un **catch-all alias**. Un catch-all alias est pratique car il reçoit les emails pour tous les utilisateurs de votre domaine.

> **Remarque**
> Avira déconseille l'utilisation d'un réglage « catch-all ». La meilleure approche est de créer un compte utilisateur séparé dans AMES pour chaque utilisateur existant. La fonction LDAP peut réduire le temps passé à cette tâche. Contactez votre partenaire Avira pour de plus amples informations.

3.3.1 Ajout d'un nouvel utilisateur

1. Pour ajouter un utilisateur manuellement, allez dans **Aperçu du domaine** et cliquez sur l'onglet **Utilisateurs**.

2. Cliquez sur **Ajouter** pour ouvrir la boîte de dialogue **Ajouter un utilisateur au domaine** :



   Chaque **Nom d'utilisateur** est considéré comme **adresse email primaire** de cet utilisateur; toute autre adresse email de cet utilisateur spécifique est considéré comme **pseudonyme**.

3. Tapez le **Nom d'utilisateur** et le **Mot de passe** pour votre nouvel utilisateur. Le mot de passe doit faire au moins 6 caractères de long. La sévérité du mot de passe s'affiche à mesure que vous le tapez :

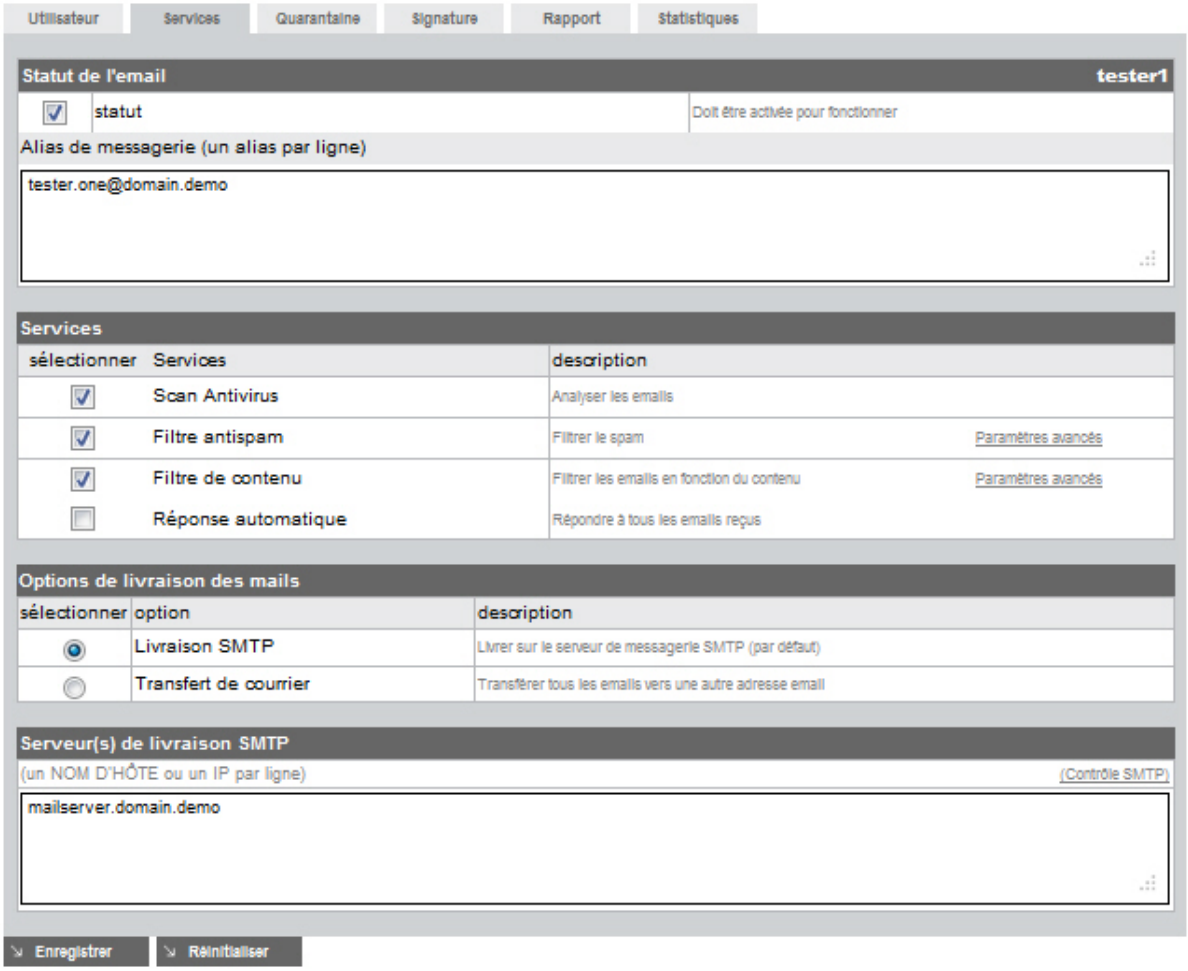
4. Si vous souhaitez que cet utilisateur soit capable de gérer les paramètres du domaine sur https://ames.avira.com, activez l'option **Admin de domaine**.

5. Vous pouvez appliquer ces paramètres à partir d'un utilisateur existant, en le sélectionnant dans la liste déroulante **Copier les paramètres depuis**.

6. Une fois terminé, cliquez sur **Enregistrer**.

   Vous serez averti que l'utilisateur est désactivé par défaut. Ceci pour vous permettre de revoir les paramètres avant qu'ils ne prennent effet.

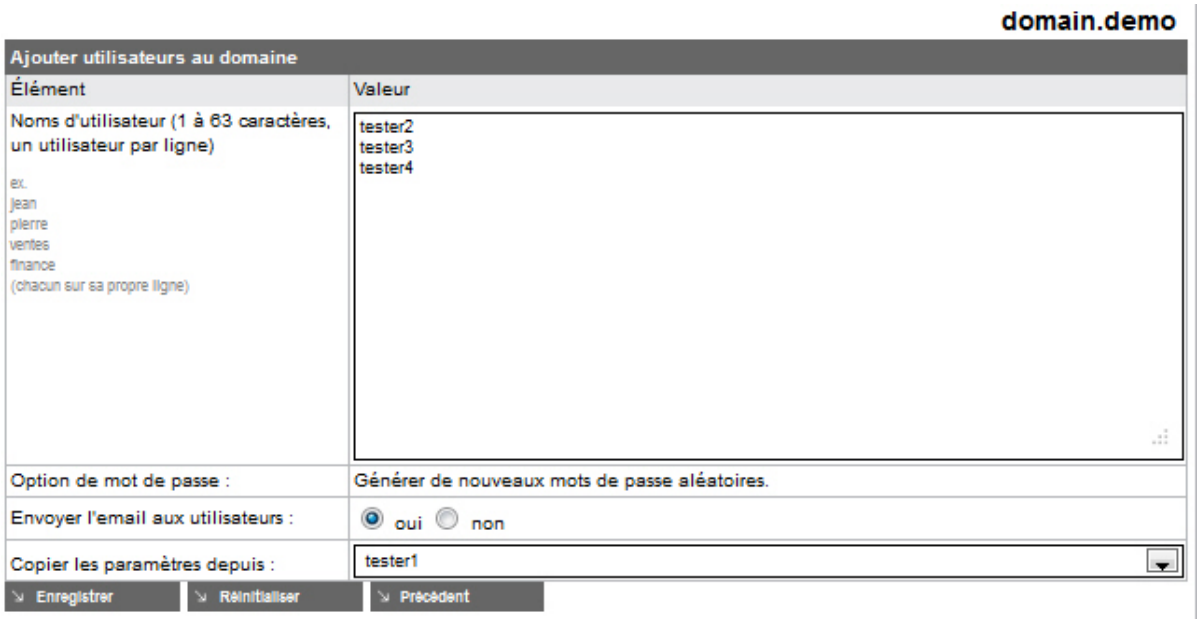
7. Pour activer l'utilisateur, cliquez sur son nom dans l'onglet **Utilisateurs** et activez l'option **statut** et les services disponibles dans l'onglet *Services* :



- **Scan Antivirus** - Les messages sont analysés à la recherche de virus.
- **Filtre antispam** - Les messages sont analysés à la recherche de spam.
- **Filtre de contenu** - Les composants du message sont analysés, en fonction des règles de contenus de la liste blanche/liste noire.
- **Réponse automatique** - Les utilisateurs sont autorisés à activer le service de réponse automatique.
- **Livraison SMTP** - Les messages sont délivrés au serveur mail SMTP.
- **Transfert de courrier** - Les messages sont transférés vers une autre adresse email.

3.3.2 Ajout d'utilisateurs multiples à un domaine (Ajout en masse)

1. Pour ajouter plusieurs utilisateurs d'un coup, allez dans **Aperçu du domaine**, cliquez sur l'onglet **Utilisateurs** et appuyez sur **Ajout en masse**.



2. Insérez les noms des nouveaux utilisateurs, un par ligne, dans la zone **Noms d'utilisateurs**.

3. Vous pouvez appliquer ces paramètres à partir d'un utilisateur existant, en le sélectionnant dans la liste déroulante **Copier les paramètres depuis**.

4. La fonction **Ajout en masse** génère des mots de passe au hasard et les envoie par email aux utilisateurs si l'option **Envoyer l'email aux utilisateurs** est réglée sur **oui**.

5. Une fois terminé, cliquez sur **Enregistrer**.

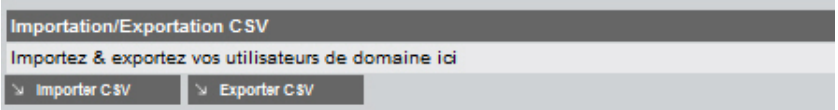
   Un message s'affiche avec la liste des utilisateurs et mots de passe ajoutée au domaine.

6. Envoyez les nouvelles données de connexion à vos nouveaux utilisateurs si l'option **Envoyer l'email aux utilisateurs** a été réglée sur **non**.

3.4 Importation/Exportation de la liste des utilisateurs du domaine

Les partenaires Avira et administrateurs de domaine AMES peuvent importer/exporter la liste des utilisateurs d'un domaine dans un fichier de type csv. Le fichier est éditable et contient les réglages pour chaque utilisateur. Il peut servir à ajouter ou modifier les réglages pour un grand nombre d'utilisateurs (mises à jour en masse).

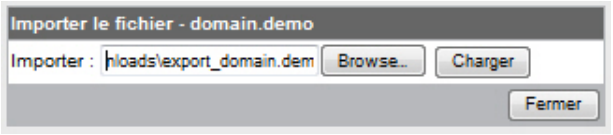
1. Pour effectuer une importation ou une exportation de la liste des utilisateurs, allez à **Aperçu du domaine**, cliquez sur l'onglet **Domaine** et descendez jusqu'à la section *Importation/Exportation CSV*.



2. Cliquez sur **Exporter CSV** et ouvrez le fichier d'exportation dans un éditeur ou enregistrez-le sur votre système.

   Vous pouvez effectuer des modifications des paramètres utilisateurs dans un tableur, selon les besoins.

3. Vous pouvez ensuite enregistrer le fichier comme .txt et le réimporter dans le domaine en cliquant sur **Importer CSV** dans l'onglet **Domaine**.



4. Dans la boîte de dialogue **Importer fichier**, sélectionnez le fichier sur votre système et cliquez sur **Charger**.

5. Vous pouvez revoir la liste des utilisateurs importés et cliquer sur **sync** pour finaliser l'importation et générer de nouveaux mots de passe aléatoires pour tous les utilisateurs.

Symboles de statut :

- utilisateur ajouté

- utilisateur modifié

- utilisateur supprimé

3.5 Ajout d'un alias d'utilisateur

Les alias d'utilisateurs peuvent être utilisés pour attribuer plusieurs adresses email à un seul utilisateur.

1. Si vous souhaitez créer un alias, sélectionnez l'utilisateur dans l'onglet **Utilisateurs**.

   L'onglet **Services** pour l'utilisateur sélectionné s'ouvre :

2. Ajoutez une ou plusieurs adresses email dans le champ **Alias de messagerie**. (ex. `tester.un@domain.demo`). Insérez chacune sur une nouvelle ligne, non séparée par d'autres caractères.

3. Cliquez sur **Enregistrer** au bas de la page une fois terminé.

Liste grise

Avertissement

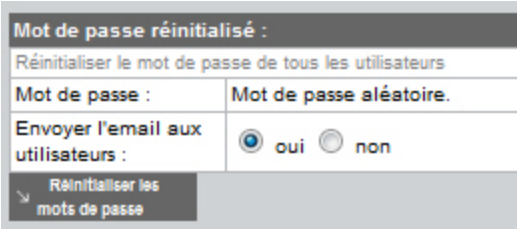
Si vous souhaitez utiliser une **adresse catch-all**, utilisez le caractère générique * (`*@domain.demo`), mais notez :
L'utilisation d'un réglage catch-all, où toutes les combinaisons de caractères devant le nom de domaine sont acceptées comme adresse email (`*@exemple.com`), rend votre domaine très vulnérable aux spams et virus. C'est pourquoi, AMES permet **la mise sur liste grise avancée** pour tous les utilisateurs catch-all. Cette technique retourne les emails des expéditeurs inconnus la première fois et les accepte uniquement à partir de la deuxième tentative. Un grand nombre de serveurs de spams n'essayant pas de renvoyer les emails refusés, la mise sur liste grise réduit sensiblement la quantité d'emails à filtrer et à analyser.

Remarque
Etant donné que le temps pris par les emails pour être redélivrés dépend du serveur mail de l'expéditeur, ce qui retarde la livraison des emails, Avira déconseille l'utilisation d'un réglage « catch-all ». La meilleure approche est de créer un compte utilisateur séparé dans AMES pour chaque utilisateur existant. La fonction **Synchronisation du domaine** peut vraiment réduire le temps passé à cette tâche.

3.6 Réinitialisation des mots de passe des utilisateurs

Les administrateurs de domaine et partenaires Avira peuvent réinitialiser les mots de passe de tous les utilisateurs d'un domaine en générant des mots de passe aléatoires.

1. Pour réinitialiser tous les mots de passe d'utilisateurs d'un domaine, allez à l'**Aperçu du domaine**, cliquez sur l'onglet **Services**, descendez jusqu'à la section **Mot de passe réinitialisé**.

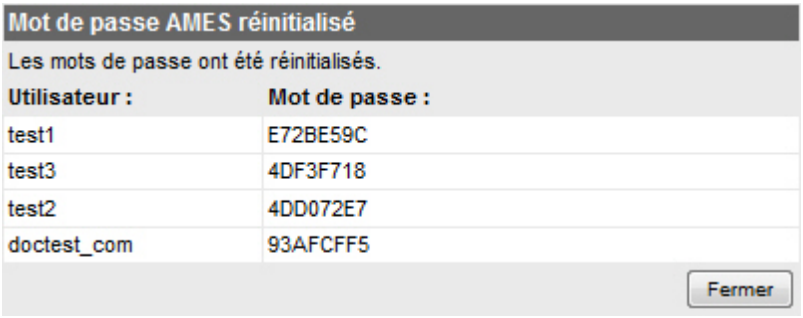


2. Laissez l'option **Envoyer l'email aux utilisateurs** activée (réglage par défaut **oui**), si vous souhaitez envoyer les nouvelles données de connexion aux utilisateurs par email.

3. Cliquez sur **Réinitialiser les mots de passe** pour générer les nouvelles données de connexion.

   Une liste des données générées s'affiche.

4. Si vous n'avez pas activé l'option **Envoyer l'email aux utilisateurs**, assurez-vous d'enregistrer cette liste et d'envoyer les données de connexion à chaque utilisateur.



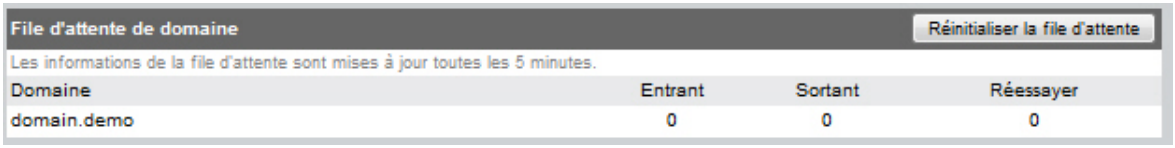
3.7 Paramètres de synchronisation (LDAP/ CSV)

Ces paramètres sont disponibles uniquement pour les partenaires Avira, en raison des conséquences possibles d'une mauvaise configuration. Contactez votre partenaire Avira pour de plus amples informations.

3.8 Informations de file d'attente de domaine

En tant que partenaire Avira ou administrateur de domaine, vous pouvez afficher les statistiques des files d'attente **Entrant**, **Sortant** et **Réessayer** par domaine.

1. Sélectionnez un domaine et cliquez sur l'onglet **Domaine**. Descendez à la section *File d'attente de domaine* :



2. Vous pouvez utiliser le bouton **Réinitialiser la file d'attente** pour vider la file d'attente d'emails.

3.9 Modification des options de livraison des mails pour un utilisateur

Vous pouvez choisir entre une livraison sur votre serveur SMTP (réglage par défaut) ou un transfert des emails à une autre adresse (au cas où il vous faudrait ce service temporairement).

1. Pour modifier les réglages de livraison des mails, sélectionnez un **Utilisateur** et allez à l'onglet **Services**.

2. Sous *Options de livraison des mails*, vous pouvez choisir entre deux méthodes :

- Activez **Livraison SMTP**.
  Sous **Serveur(s) de livraison SMTP**, vous pouvez ajouter un ou plusieurs hôtes ou adresses IP auxquels AMES délivrera les emails.
- Activez **Transfert de courrier**.
  Sous **Transférez votre email à cette adresse**, vous pouvez taper une ou plusieurs adresses email auxquelles AMES délivrera vos emails.

3. Une fois terminé, cliquez sur **Enregistrer**.

3.10 Personnaliser les signatures d'emails

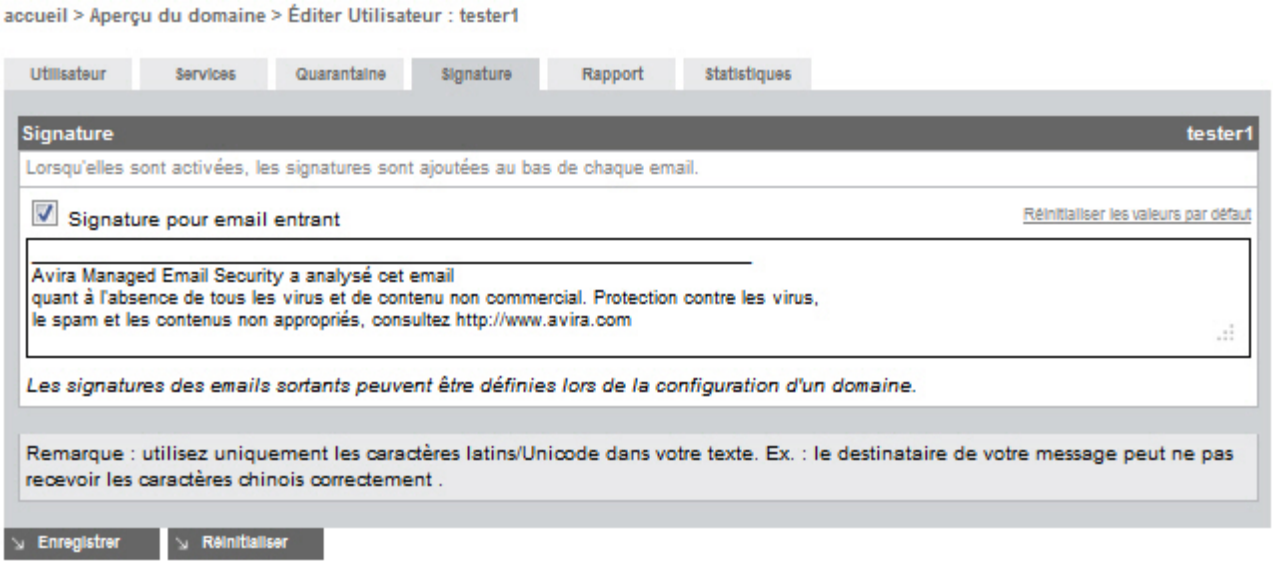
AMES vous permet d'ajouter un message personnalisé (signature) au bas d'un email entrant ou sortant.

> **Remarque**
> Utilisez exclusivement des caractères standard Western Latin/Unicode dans le texte de signature.

Ajout d'une signature à des emails entrants

Vous pouvez ajouter une signature **spécifique à l'utilisateur** à des emails entrants.

1. Sélectionnez l'**Utilisateur** pour lequel vous souhaitez ajouter une signature et allez dans l'onglet **Signature**.



2. Activez l'option **Signature pour email entrant** et rédigez le texte dans la zone prévue.

   -OU-

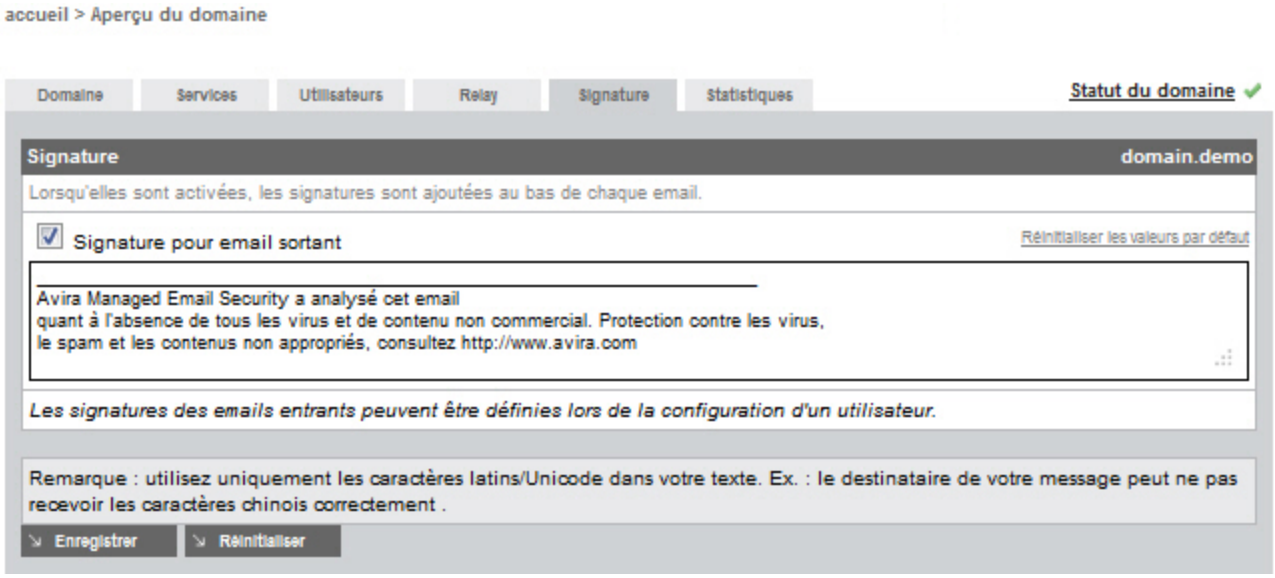
   Cliquez sur le lien **Réinitialiser les valeurs par défaut** si vous souhaitez utiliser une signature standard.

3. Cliquez sur **Enregistrer**.

Ajouter une signature à des emails sortants

Vous pouvez ajouter une signature **spécifique au domaine** aux emails sortants, dans le cas où vous utilisez le service relais (voir 2.4 Analyse des emails sortants - page 9).

1. Sélectionnez le **Domaine** pour lequel vous souhaitez ajouter une signature et allez dans l'onglet **Signature**.



2. Activez l'option **Signature pour email sortant** et rédigez le texte dans la zone prévue.

   -OU-

   Cliquez sur le lien **Réinitialiser les valeurs par défaut** si vous souhaitez utiliser une signature standard.

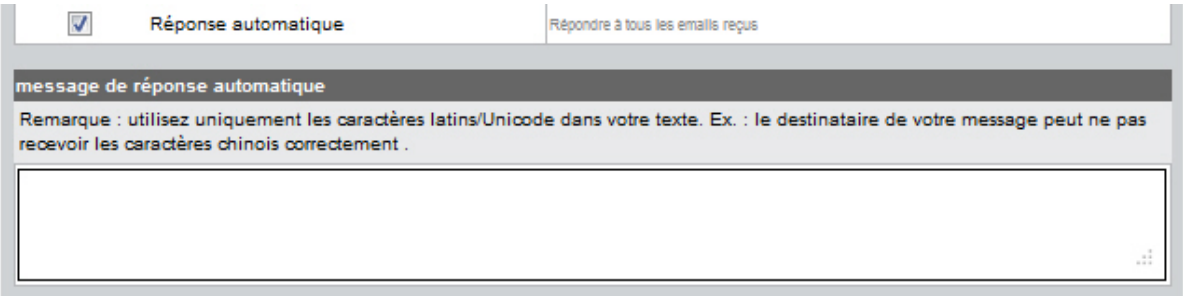
3. Cliquez sur **Enregistrer**.

3.11 Configurer une réponse automatique

1. Pour configurer un message de réponse automatique aux emails reçus par un utilisateur (par exemple, un message d'absence), sélectionnez l'**Utilisateur**, allez à **Services** et activez le service **Réponse automatique** :

Remarque
Si le service **Réponse automatique** n'est pas listé pour l'utilisateur sélectionné, le service doit être activé par un administrateur du domaine ou un partenaire Avira (voir 3.2 Configuration des services disponibles pour les utilisateurs finaux - page 11).

2. Tapez le message de réponse (avec des caractères standard Western Latin/Unicode) dans la zone de texte de **message de réponse automatique**.



3. Cliquez sur **Enregistrer** pour appliquer la modification.

4. Gestion de la quarantaine

4.1 Configuration des filtres d'emails

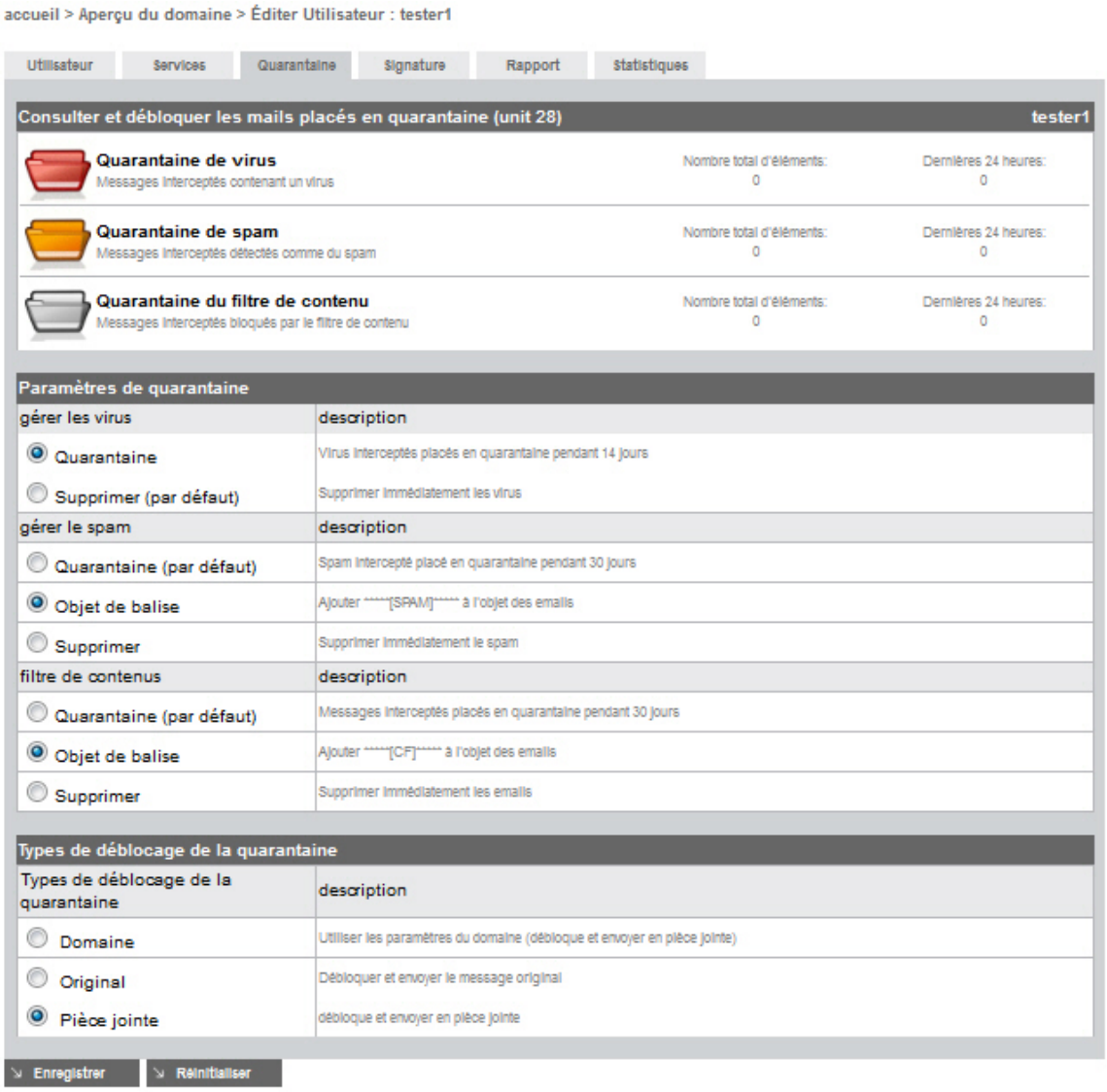
AMES intègre une variété d'outils de filtrage et d'analyse des emails. Vous pouvez configurer votre compte AMES afin qu'il supprime les emails infectés immédiatement, qu'il les envoie en quarantaine ou simplement qu'il place une balise dans leur objet. En outre, vous pouvez régler le niveau d'heuristique du contrôle des spams, définir des règles avancées antispam et de filtrage des contenus.

Remarque
En fonction de la politique de sécurité de leur entreprise, les administrateurs du domaine peuvent configurer les filtres, les quarantaines et les rapports et désactiver ces options pour les utilisateurs finaux.

4.1.1 Traitement des spams et virus interceptés

Par défaut, AMES envoie tous les emails de spam et filtrés en quarantaine. Vous pouvez choisir une autre réaction, telle que mettre une balise à l'email et le délivrer à la boîte de réception, ou même le supprimer immédiatement.

1. Choisissez un **Utilisateur** pour lequel vous souhaiteriez configurer le traitement des spams et virus et cliquez sur l'onglet **Quarantaine**.



2. Sélectionnez l'action que vous souhaitez appliquer aux emails infectés, aux spams ou au contenu filtré :

   - Sous **gérer les virus** : sélectionnez **Quarantaine** pour que les emails infectés soient mis en quarantaine pendant 14 jours, puis supprimés ; ou sélectionnez **Supprimer**, pour supprimer immédiatement les emails infectés (réglage par défaut).
   - Sous **gérer le spam** : sélectionnez **Quarantaine** pour que les emails de spam soient mis en quarantaine pendant 30 jours, puis supprimés (réglage par défaut) ; ou sélectionnez **Objet de balise** pour repérer l'objet des emails de spam avec `******[SPAM]*******` dans votre boîte d'entrée ; ou sélectionnez **Supprimer** pour supprimer immédiatement les emails de spam.
   - Sous **filtre de contenus** : sélectionnez **Quarantaine** pour que les emails filtrés soient mis en quarantaine pendant 30 jours, puis supprimés (réglage par défaut) ; ou sélectionnez **Objet de balise** pour repérer l'objet des emails filtrés avec `******[CF]*******` dans votre boîte d'entrée ; ou sélectionnez **Supprimer** pour supprimer immédiatement les emails filtrés.

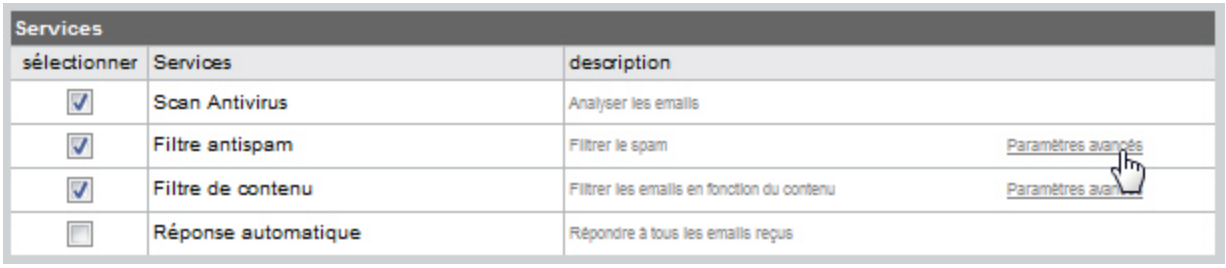
3. A leur sortie de la quarantaine, les emails bloqués peuvent être livrés comme pièce jointe ou message original. Pour définir ce réglage en fonction de l'utilisateur, utilisez l'option **Types de déblocage de la quarantaine** :

   - **Domaine** - Conserver le réglage défini par l'administrateur du domaine pour la totalité du domaine (voir 3.1 Définition des paramètres généraux du domaine - page 10).
   - **Original** - Envoyer le message d'origine dans la boîte de réception de l'utilisateur.
   - **Pièce jointe** - Envoyer le message bloqué sous forme de pièce jointe à un email d'avertissement dans la boîte de réception de l'utilisateur.

4. Cliquez sur **Enregistrer** pour enregistrer les réglages.

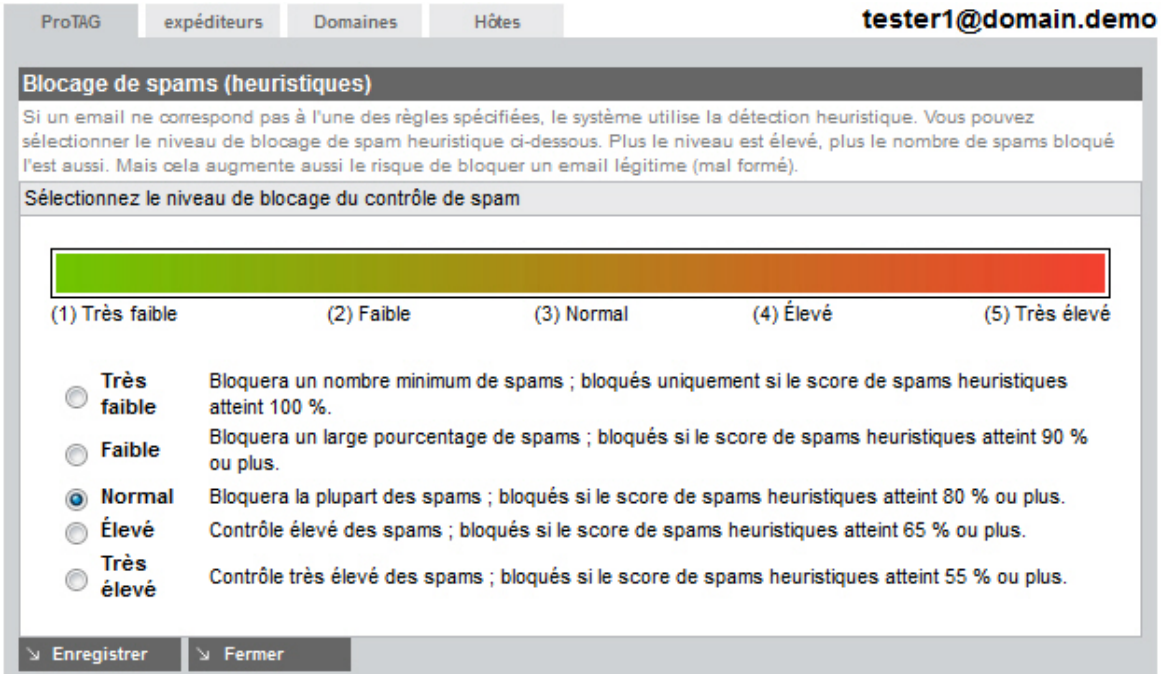
4.1.2 Ajustement des réglages des filtres

Si vous souhaitez modifier les réglages du filtre antispam et/ou du filtre de contenu, sélectionnez un **Utilisateur**, allez à l'onglet **Services** et cliquez sur **Paramètres avancés** pour le filtre que vous souhaitez ajuster.



Filtre antispam

Sur la page **Paramètres avancés**, cliquez sur **ProTAG**. Ici, vous pouvez définir le niveau de blocage pour le contrôle antispam heuristique qui est appliqué à vos emails entrants.



Il existe cinq niveaux de sévérité pour le contrôle antispam, en fonction du score de spam heuristique :

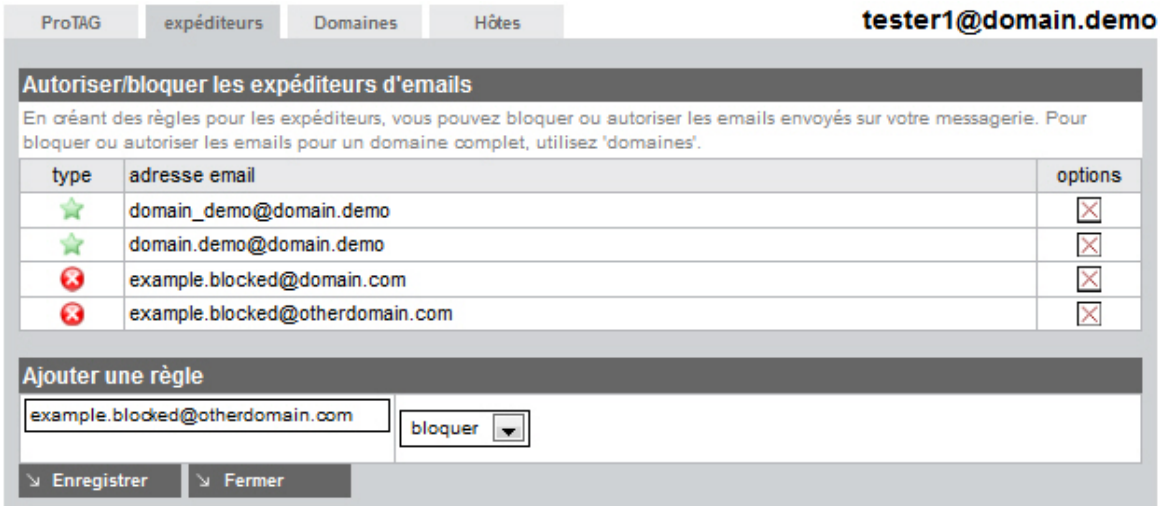
- **Très faible** - ne bloque que les messages avec un score de spam heuristique de 100 %.
- **Faible** - ne bloque que les messages avec un score de spam heuristique supérieur à 90 %.
- **Normal** - ne bloque que les messages avec un score de spam heuristique supérieur à 80 %.
- **Élevé** - bloque les messages avec un score de spam heuristique supérieur à 65 %.
- **Très élevé** - bloque les messages avec un score de spam heuristique supérieur à 55 %.

Le réglage par défaut est **Normal**.

> **Remarque**
> Pour les organisations avec un taux normal de spams, nous conseillons le niveau **Normal**. Le risque de régler le filtre antispam sur **Élevé** ou **Très élevé** est que des emails légitimes ayant des caractéristiques de spams soient bloqués. C'est pourquoi nous vous conseillons de surveiller votre quarantaine de spam régulièrement et de programmer un rapport de spams quotidien.

Avec les réglages du filtre antispam, vous pouvez bloquer ou autoriser certains expéditeurs d'emails, domaines ou hôtes.

1. Par exemple, pour ajouter des règles pour les expéditeurs d'emails, cliquez sur l'onglet **Expéditeurs**.



2. Insérez l'adresse email de l'expéditeur dans le champ situé sous *Ajouter une règle*. (ex. `exemple.bloqué@autredomaine.com`).

3. Sélectionnez le type de règle : **bloquer** ou **autoriser**.

4. Cliquez sur **Enregistrer** pour ajouter la règle.

Les règles sont listées sous *Autoriser/bloquer les expéditeurs d'emails*, avec les symboles de types :
- bloquer (liste noire) ou
- autoriser (liste blanche).

Pour supprimer une règle, cliquez sur le **X** dans la colonne **options** et cliquez sur **OK** dans la fenêtre contextuelle.

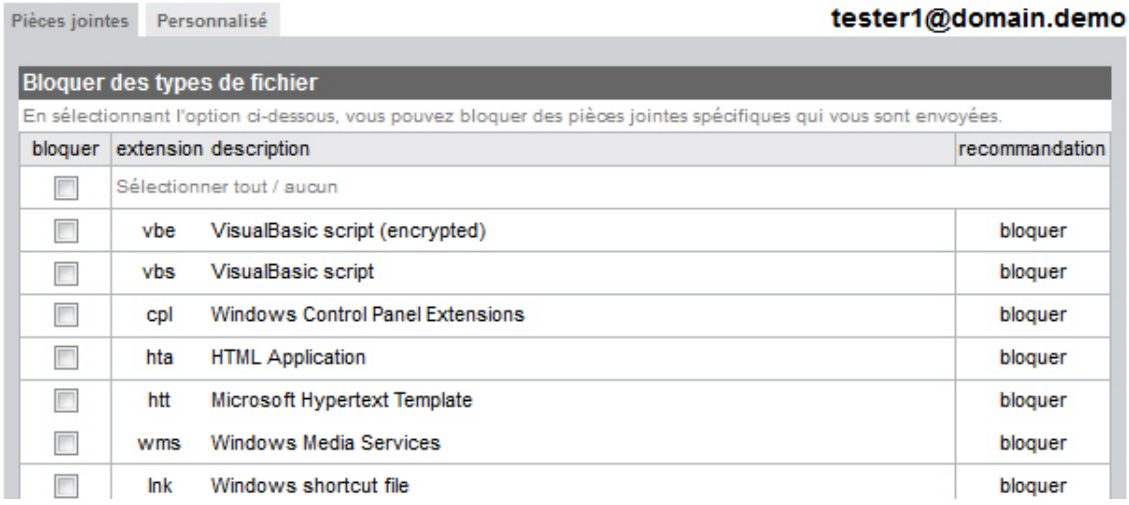
Utilisez les onglets **Domaines** et **Hôtes** pour ajouter des règles afin de bloquer ou d'autoriser certains domaines et adresses IP. Cette procédure est similaire à celle pour les **Expéditeurs**.

Remarque
Les règles du filtre antispam sont également ajoutées lorsque vous utilisez les options de liste blanche **Expéditeur sans danger** ou **Domaine sans danger** dans le *Résumé de quarantaine d'emails*.
Voir « Options de liste blanche » - page 31.

Filtre de contenu

Dans les réglages du filtre de contenu, vous pouvez définir des règles pour les pièces jointes ou des règles personnalisées :

- **Pièces jointes :** cochez les cases de la première colonne de la liste des extensions pour **bloquer** certains types de fichiers.

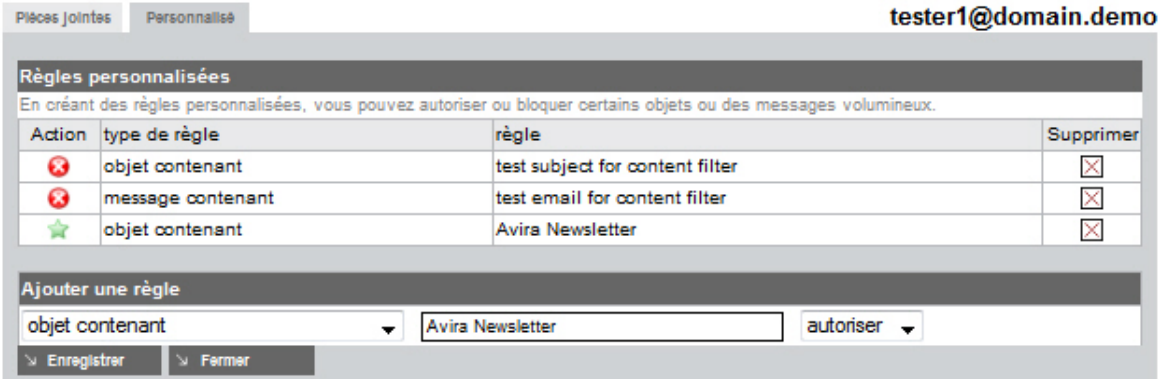


La liste contient les recommandations suivantes :

- *bloquer* : vous devriez bloquer ce type de pièce jointe.
- *bloquer en cas de doute* : si vous n'êtes pas sûr de vouloir autoriser ce type de pièce jointe, nous vous conseillons de le bloquer.
- *ne pas bloquer* : pièces jointes acceptées par défaut ; vous pouvez les bloquer si vous le souhaitez.

Pour faciliter la sélection, vous pouvez utiliser l'option **Sélectionner tout/aucun** : utilisez-la pour sélectionner/désélectionner toutes les extensions, puis cliquez sur celles que vous souhaitez bloquer/autoriser.

- **Personnalisé :** vous pouvez créer vos propres règles pour **bloquer** ou **autoriser** des emails :



Pour ajouter une règle personnalisée :

1. Sélectionnez un critère de filtre dans la liste déroulante :

   - **objet contenant :** autorise ou bloque les emails contenant un certain objet.
   - **message contenant :** autorise ou bloque les emails contenant une certaine chaîne.
   - **taille du message supérieure à :** bloque les emails excédent une taille de message maximum en kb.

2. Tapez le texte que vous souhaitez filtrer (ex. `Avira Newsletter`) ou la taille maximum des messages (ex. `5120`).

3. Sélectionnez le type de règle : **bloquer** ou **autoriser**.

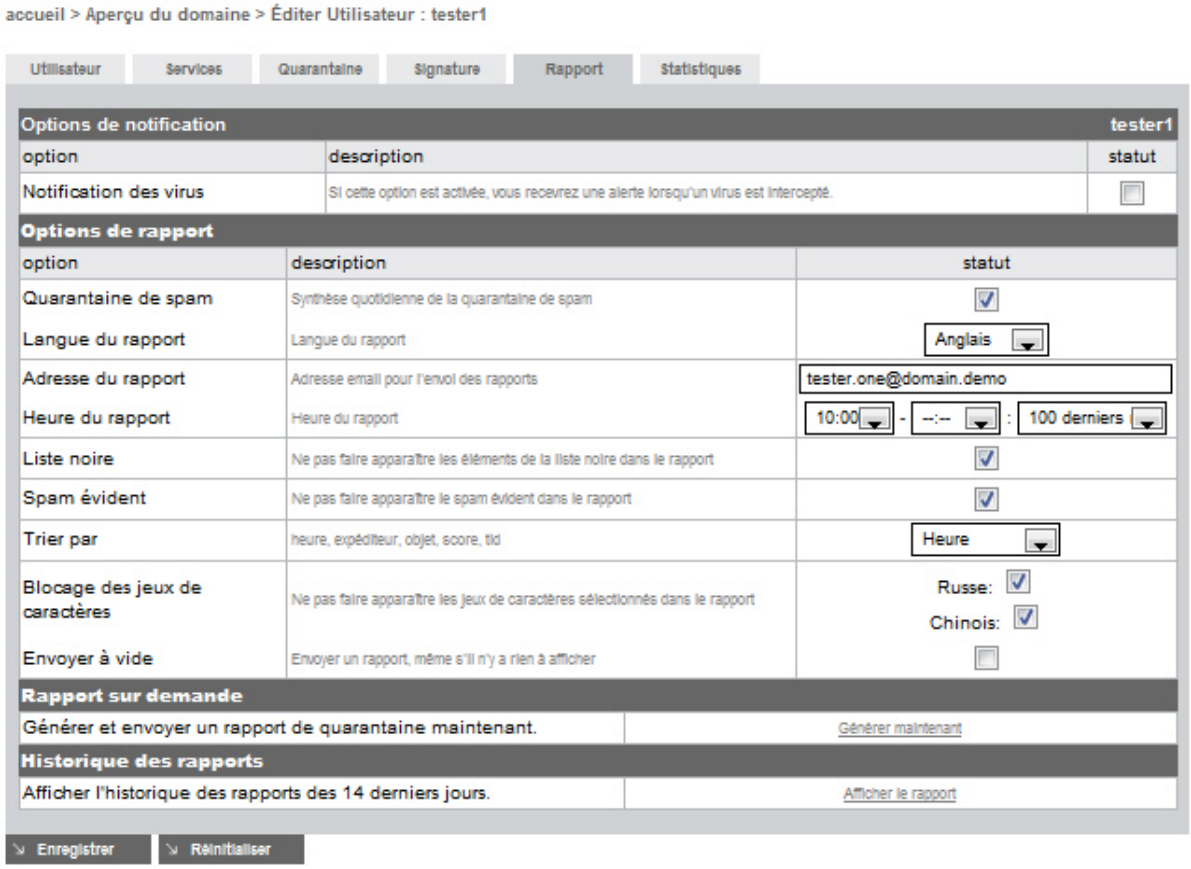
4. Cliquez sur **Enregistrer** pour ajouter la règle.

   Les règles sont listées sous *Règles personnalisées*, avec les symboles de types :
   bloquer (liste noire) ou
   autoriser (liste blanche).

Pour supprimer une règle, cliquez sur le **X** dans la colonne **Supprimer** et cliquez sur **OK** dans la fenêtre contextuelle.

4.2 Définition des notifications de virus et de spam

1. Pour programmer un rapport, sélectionnez un **Utilisateur** puis cliquez sur l'onglet **Rapport**.



2. Activez **Notification des virus** pour recevoir un avertissement par email dès qu'un virus est intercepté.

3. Activez **Quarantaine de spam** pour recevoir un résumé quotidien des spams interceptés, en fonction des réglages effectués sous *Options de rapport* :

- **Langue du rapport** - vous pouvez actuellement choisir entre : Anglais, Allemand, Espagnol, Français et Néerlandais.
- **Adresse du rapport** - insérez une adresse email à laquelle AMES enverra les notifications de virus et résumés de spams.
- **Heure du rapport** - par défaut, AMES envoie le résumé des spams deux fois par jour (p. ex. `08:00`, `16:00`). Vous pouvez sélectionner différentes heures ou désactiver l'une d'elles.
  Autres options pour les heures de rapport :
  - `Dernier rapport 100` - liste de 100 éléments depuis le dernier rapport.
  - `Dernier rapport 500` - liste de 500 éléments depuis le dernier rapport.
  - `100 derniers éléments` - liste des 100 derniers éléments.

- `500 derniers éléments` - liste des 500 derniers éléments.

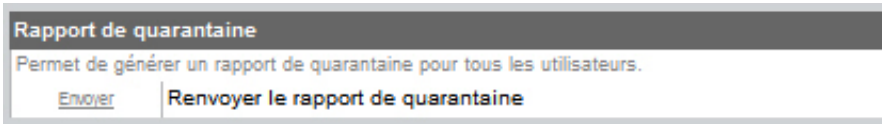
- **Liste noire** - AMES n'affiche pas les éléments sur liste noire dans le résumé si vous activez cette option.
- **Spam évident** - AMES n'affiche pas les éléments avec un score spam élevé dans le résumé si vous activez cette option.
- **Trier par** - sélectionnez un critère pour trier la liste de résumé : `Heure`, `Expéditeur`, `Objet`, `Score`, `TLD` (domaine niveau supérieur).
- **Blocage des jeux de caractères** - AMES n'affiche pas les jeux de caractères **russe** ou **chinois** dans le résumé si vous activez ces options.
- **Envoyer à vide** - AMES envoie un rapport, même s'il n'y a rien à afficher.

4. Une fois terminé, cliquez sur **Enregistrer**.

Avertissement
Nous conseillons de faire générer un rapport quotidien par AMES, surtout si vous venez juste de commencer à utiliser AMES ou si vous utilisez des réglages de filtrage stricts des spams.

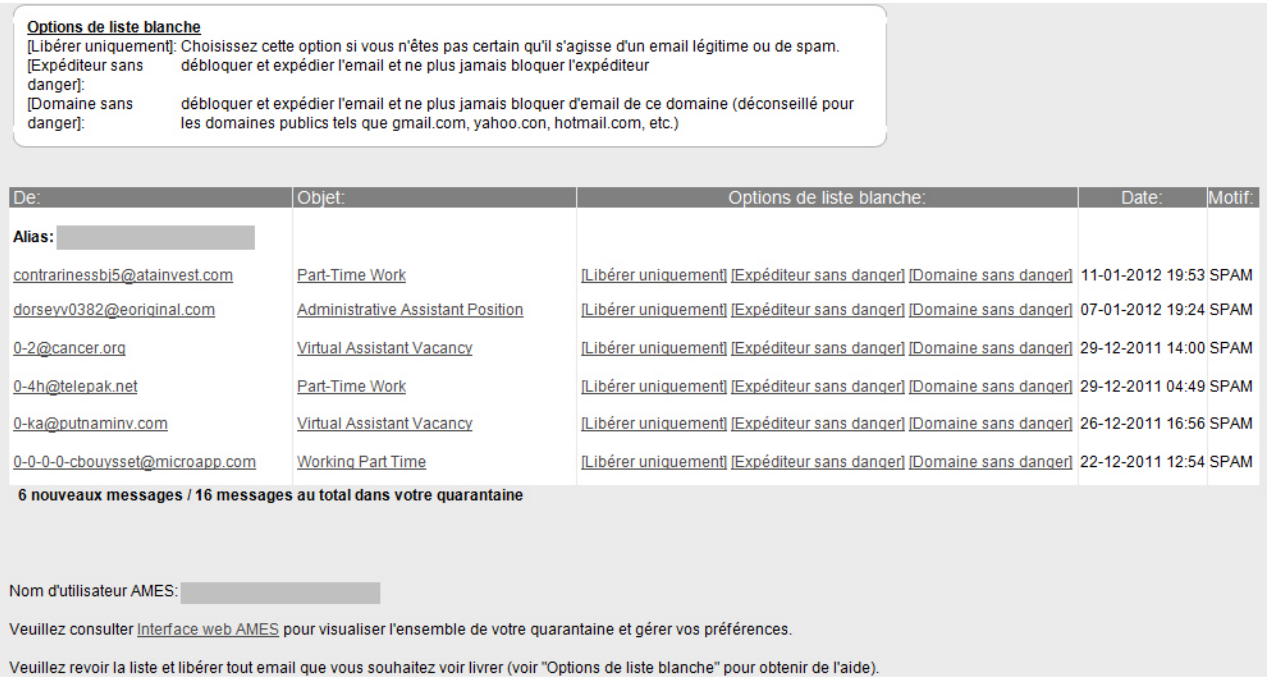
5. Cliquez sur **Générer maintenant** si vous souhaitez recevoir le résumé de quarantaine par email immédiatement. Pour afficher un historique de rapports des 14 derniers jours, cliquez sur **Afficher le rapport**.

En tant que partenaire Avira ou administrateur de domaine AMES, vous pouvez générer un rapport de quarantaine et l'envoyer à tous les utilisateurs d'un domaine : allez à l'**Aperçu du domaine > Services**, descendez jusqu'à la section *Rapport de quarantaine* et cliquez sur **Envoyer**.



4.3 Gestion des quarantaines directement à partir de votre compte email

Une fois le rapport de résumé quotidien activé, l'utilisateur reçoit un email chaque jour, comme programmé, avec la liste des éventuels nouveaux messages de spam.



Options de liste blanche
[Libérer uniquement]: Choisissez cette option si vous n'êtes pas certain qu'il s'agisse d'un email légitime ou de spam.
[Expéditeur sans danger]: débloquer et expédier l'email et ne plus jamais bloquer l'expéditeur
[Domaine sans danger]: débloquer et expédier l'email et ne plus jamais bloquer d'email de ce domaine (déconseillé pour les domaines publics tels que gmail.com, yahoo.con, hotmail.com, etc.)

De:	Objet:	Options de liste blanche:	Date:	Motif:
Alias:				
contrarinessbj5@atainvest.com	Part-Time Work	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	11-01-2012 19:53	SPAM
dorseyv0382@eoriginal.com	Administrative Assistant Position	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	07-01-2012 19:24	SPAM
0-2@cancer.org	Virtual Assistant Vacancy	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	29-12-2011 14:00	SPAM
0-4h@telepak.net	Part-Time Work	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	29-12-2011 04:49	SPAM
0-ka@putnaminv.com	Virtual Assistant Vacancy	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	26-12-2011 16:56	SPAM
0-0-0-0-cbouysset@microapp.com	Working Part Time	[Libérer uniquement] [Expéditeur sans danger] [Domaine sans danger]	22-12-2011 12:54	SPAM

6 nouveaux messages / 16 messages au total dans votre quarantaine

Nom d'utilisateur AMES:

Veuillez consulter Interface web AMES pour visualiser l'ensemble de votre quarantaine et gérer vos préférences.

Veuillez revoir la liste et libérer tout email que vous souhaitez voir livrer (voir "Options de liste blanche" pour obtenir de l'aide).

Options de liste blanche

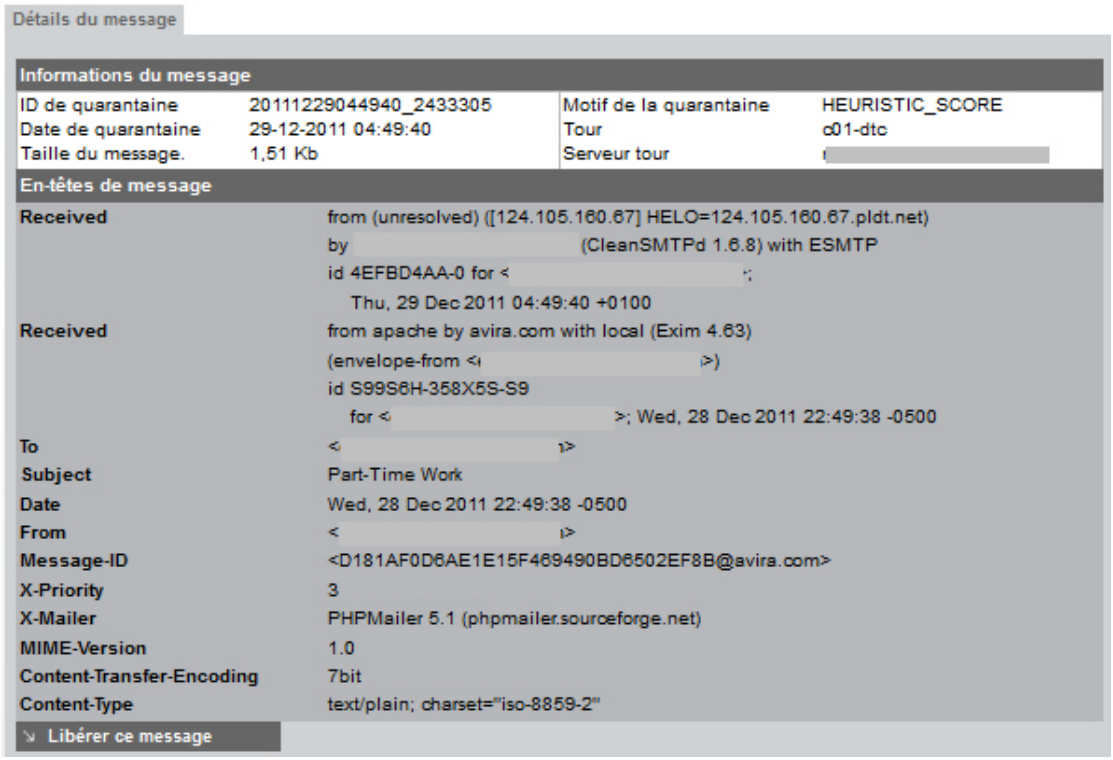
Vous pouvez gérer votre quarantaine directement depuis votre client d'email, en utilisant les liens dans la colonne **Options de liste blanche** du résumé de quarantaine :

- Cliquez sur **Libérer uniquement** pour délivrer l'email en quarantaine dans votre boîte de réception.
- Cliquez sur **Expéditeur sans danger** pour délivrer l'email en quarantaine dans votre boîte de réception et ajouter l'expéditeur à la liste blanche de votre filtre antispam AMES, de manière que l'expéditeur ne soit plus jamais bloqué.
- Cliquez sur **Domaine sans danger** pour délivrer l'email en quarantaine dans votre boîte de réception et ajouter l'expéditeur à la liste blanche de votre filtre antispam AMES, de manière que le domaine ne soit plus jamais bloqué.

Avertissement
Il est déconseillé d'utiliser l'option **Domaine sans danger** pour les domaines publics, tels que *gmail.com*, *yahoo.com*, *hotmail.com*, etc.

Si vous souhaitez afficher votre quarantaine entière ou gérer vos préférences, vous pouvez cliquer sur le lien menant à l'**Interface web AMES** qui ouvre la page de connexion à votre compte AMES.

Vous pouvez d'abord vérifier les détails du message en quarantaine en cliquant sur son objet (ex. `Part-Time Work`) dans la colonne **Objet** du résumé de quarantaine.


Détails du message

Informations du message

ID de quarantaine	20111229044940_2433305	Motif de la quarantaine	HEURISTIC_SCORE
Date de quarantaine	29-12-2011 04:49:40	Tour	c01-dtc
Taille du message.	1,51 Kb	Serveur tour	

En-têtes de message

Received	from (unresolved) ([124.105.160.67] HELO=124.105.160.67.pldt.net) by (CleanSMTPd 1.6.8) with ESMTP id 4EFBD4AA-0 for <; Thu, 29 Dec 2011 04:49:40 +0100
Received	from apache by avira.com with local (Exim 4.63) (envelope-from <>) id S99S6H-358X5S-S9 for <>; Wed, 28 Dec 2011 22:49:38 -0500
To	<>
Subject	Part-Time Work
Date	Wed, 28 Dec 2011 22:49:38 -0500
From	<>
Message-ID	<D181AF0D6AE1E15F469490BD6502EF8B@avira.com>
X-Priority	3
X-Mailer	PHPMailer 5.1 (phpmailer.sourceforge.net)
MIME-Version	1.0
Content-Transfer-Encoding	7bit
Content-Type	text/plain; charset="iso-8859-2"

Libérer ce message

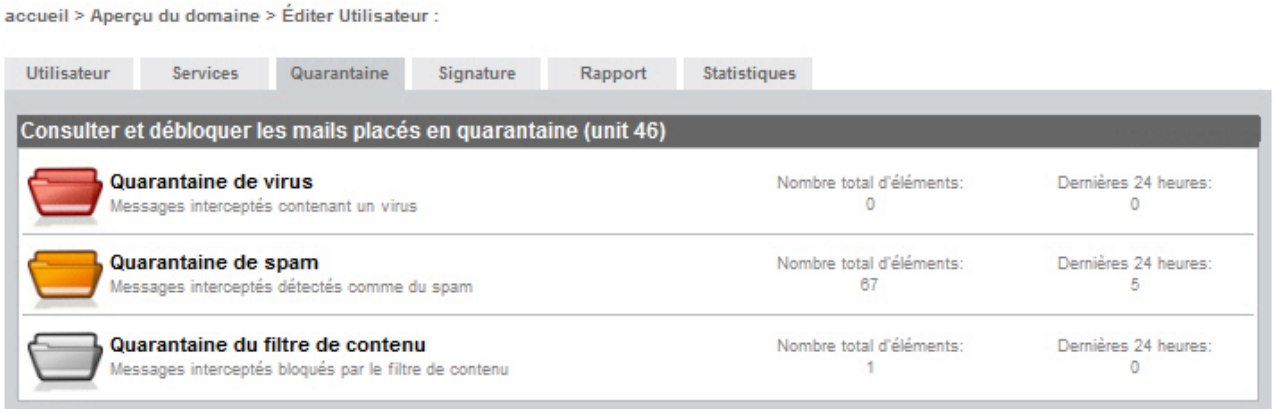
Après avoir vérifié les détails du message, tels que *Motif de la quarantaine* et *En-têtes de message*, vous pouvez toujours décider de libérer le message de la quarantaine en, cliquant sur **Libérer ce message**.

Si la fonction **Notification des virus** est activée, l'utilisateur reçoit un avertissement par email dès qu'un virus est détecté dans un message entrant. L'avertissement contient des détails sur le message infecté et un lien vers la description du logiciel malveillant sur le site web d'Avira.

L'utilisateur peut vérifier la **Quarantaine de virus** dans le compte AMES pour supprimer ou libérer l'email en quarantaine dans les 14 jours.

4.4 Gestion des quarantaines à partir de votre compte AMES

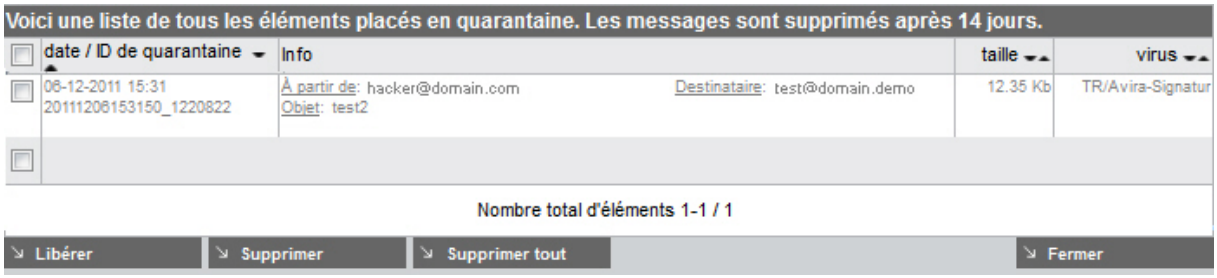
Pour ouvrir la quarantaine, sélectionnez un **Utilisateur** et allez dans l'onglet **Quarantaine**.



AMES dispose de trois quarantaines pour différents types de filtres. Cliquez sur le nom de chaque quarantaine puis vérifiez son contenu.

Quarantaine de virus

Si votre compte est configuré pour mettre en quarantaine les emails infectés pendant 14 jours, la **Quarantaine de virus** archive tous les emails avec des signatures de virus.



Pour supprimer des emails spécifiques, sélectionnez les éléments dans la liste et cliquez sur **Supprimer.** Pour supprimer tous les messages dans cette quarantaine, cliquez sur **Supprimer tout**. AMES supprimera automatiquement les emails infectés de plus de 14 jours.

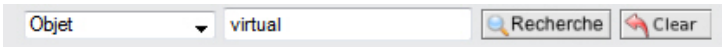
Avertissement
Si vous doutez qu'un email spécifique contienne un virus, ne le libérez pas. Le filtrage de virus AMES fait rarement des erreurs. Dans le cas où vous décideriez qu'un email n'est pas infecté, sélectionnez-le et cliquez sur **Libérer** pour le délivrer à votre boîte de réception.

Quarantaine de spam

Si votre compte est configuré pour mettre en quarantaine les emails de spam pendant 30 jours, la **Quarantaine de spam** archive tous les emails de spam interceptés.

Pour supprimer des emails spécifiques, sélectionnez les éléments dans la liste et cliquez sur **Supprimer.** Pour supprimer tous les messages dans cette quarantaine, cliquez sur **Supprimer tout**. AMES supprimera automatiquement les emails de spam après 30 jours.

Vous pouvez aussi filtrer la liste par ID, expéditeur, destinataire ou objet, grâce à la fonction **Recherche** : sélectionnez le critère de filtre dans la liste déroulante (**ID de quarantaine**, **Expéditeur**, **Destinataire**, **Objet**), insérez la chaîne que vous recherchez (ex. `viagra`) et appuyez sur **Recherche**. Si vous souhaitez supprimer la chaîne de filtre et retourner à la liste initiale, cliquez sur **Supprimer**.



Pour libérer les emails sélectionnés de la quarantaine :

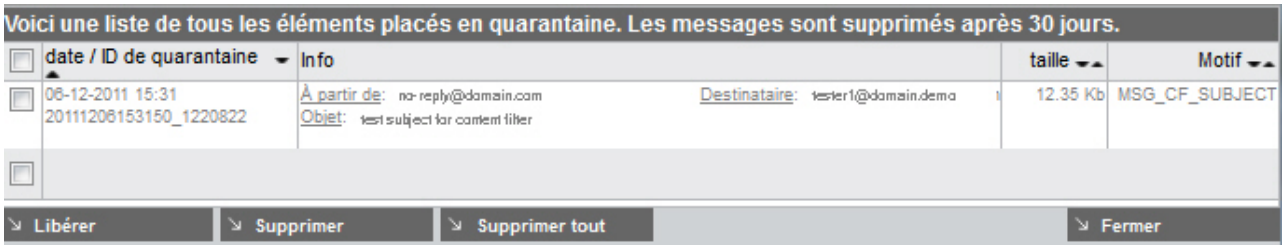
- Cliquez sur **Libérer** pour délivrer l'email sélectionné dans votre boîte de réception.
- Cliquez sur **Libérer et retenir comme non spam** pour délivrer les emails sélectionnés à votre boîte de réception et ne plus identifier les emails en provenance de ces expéditeurs comme du spam. Notez que cette action réduit l'efficacité du filtrage antispam.

- Cliquez sur **Libérer aux administrateurs** pour délivrer les emails sélectionnés à votre administrateur de domaine qui peut les vérifier pour vous.

> **Remarque**
> Vous pouvez totalement vous fier aux réglages par défaut d'AMES, mais, si vous le souhaitez, vous pouvez les personnaliser. Si vous configurez le filtre antispam à un niveau trop élevé, votre quarantaine de spam pourrait aussi intercepter **ham**. 'Ham' est faussement identifié comme spam. Si vous obtenez 'ham' dans votre quarantaine ou si vous recevez des emails faussement identifiés comme spam dans votre client email, vérifiez les Paramètres avancés du filtre antispam (voir « Filtre antispam » - page 25).

Quarantaine du filtre de contenu

Dans la **Quarantaine du filtre de contenu** vous trouverez tous les emails bloqués en raison de leur taille, de la pièce jointe ou de vos propres règles.



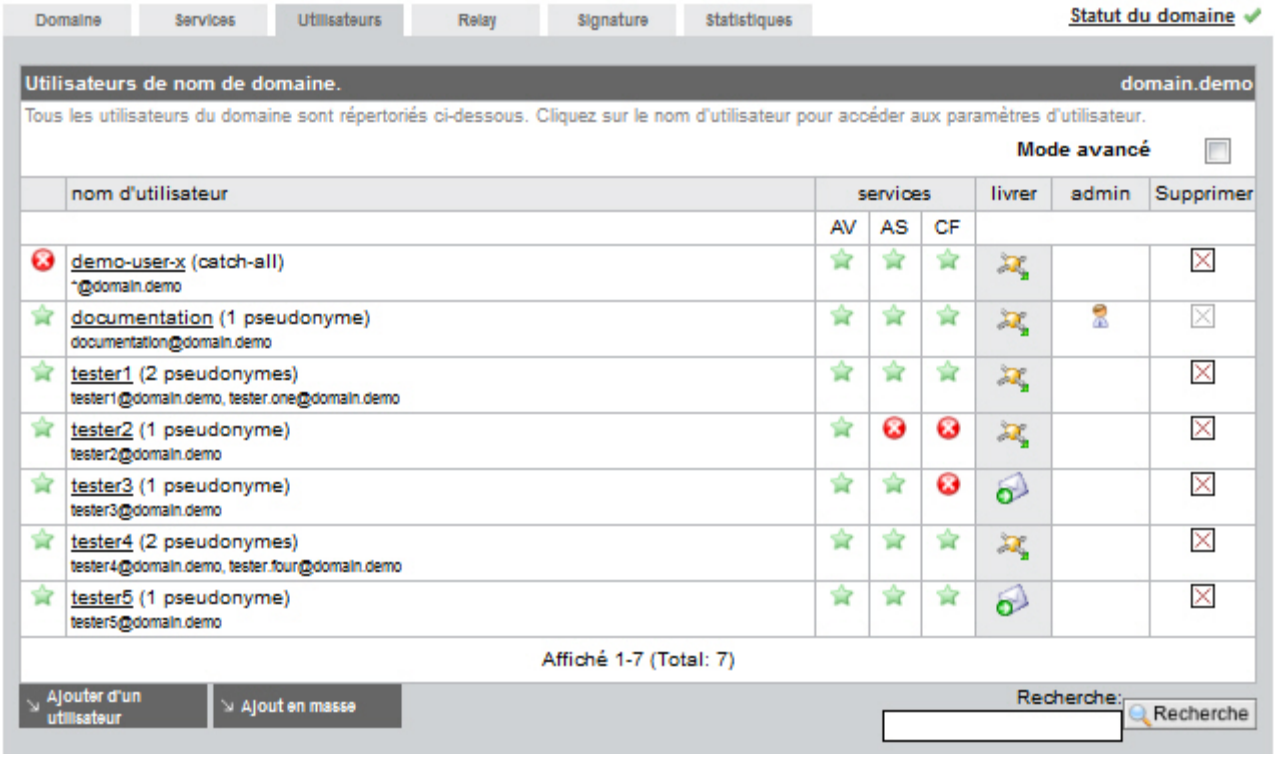
Si vous décidez de délivrer un email sélectionné à votre boîte de réception, cliquez sur **Libérer.**

Pour supprimer des emails spécifiques, sélectionnez les éléments dans la liste et cliquez sur **Supprimer.** Pour supprimer tous les messages dans cette quarantaine, cliquez sur **Supprimer tout**. AMES supprimera automatiquement les emails au contenu bloqué après 30 jours.

5. Gestion des utilisateurs

En tant que partenaire Avira ou administrateur de domaine AMES, vous pouvez gérer tous les utilisateurs d'un domaine dans **Aperçu du domaine** à l'onglet **Utilisateurs**.

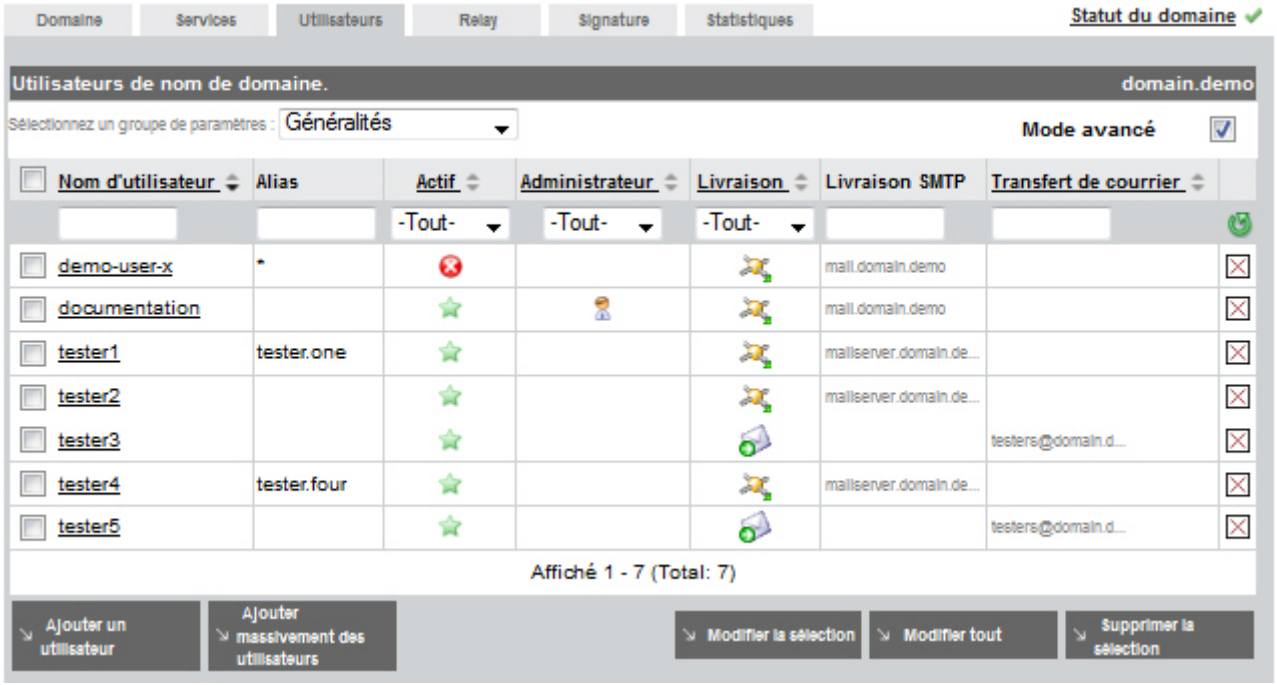
La vue par défaut affiche une liste des utilisateurs et de l'état des services pour chaque utilisateur :



- utilisateur actif ou inactif ;
- nom d'utilisateur et alias (un clic sur un nom d'utilisateur vous amène au niveau utilisateur de l'interface AMES) ;
- services actifs : Filtre à virus (AV), Filtre antispam (AS), Filtre de contenu (CF) ;
- méthode de livraison des emails (SMTP ou Transfert) ;
- symbole pour les administrateurs du domaine .

5.1 Gestion des utilisateurs en mode avancé

Si vous activez l'option **Mode avancé**, vous pouvez facilement configurer les services pour un ou plusieurs utilisateur(s) en trois étapes seulement.



1. **Sélectionnez d'abord le groupe de paramètres** dans la liste déroulante au-dessus du tableau :

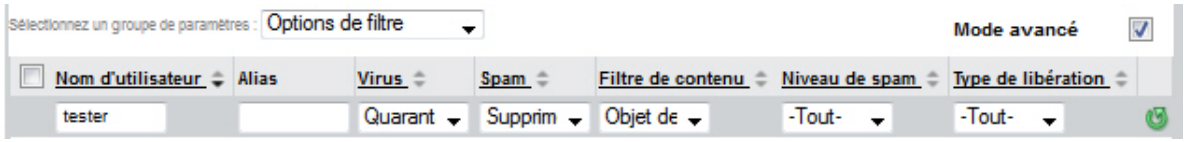
   - Généralités
   - Services
   - Options de filtre
   - Liste noire
   - Liste blanche
   - Rapport général
   - Rapport de contenu

2. **Puis, sélectionnez les utilisateurs que vous souhaitez modifier** :

   Cochez les cases de la première colonne pour sélectionner les utilisateurs. Vous pouvez utiliser la case à cocher dans l'en-tête de tableau pour sélectionner ou désélectionner tous les utilisateurs.

   Pour trier la liste des utilisateurs en fonction du contenu d'une colonne, cliquez sur l'en-tête de colonne une ou deux fois : l'une des deux flèches grises de l'en-tête devient noire pour indiquer l'ordre de tri croissant ou décroissant.

Pour filtrer la liste au moyen de certains critères, utilisez un ou plusieurs champs au-dessous des en-têtes de colonnes.

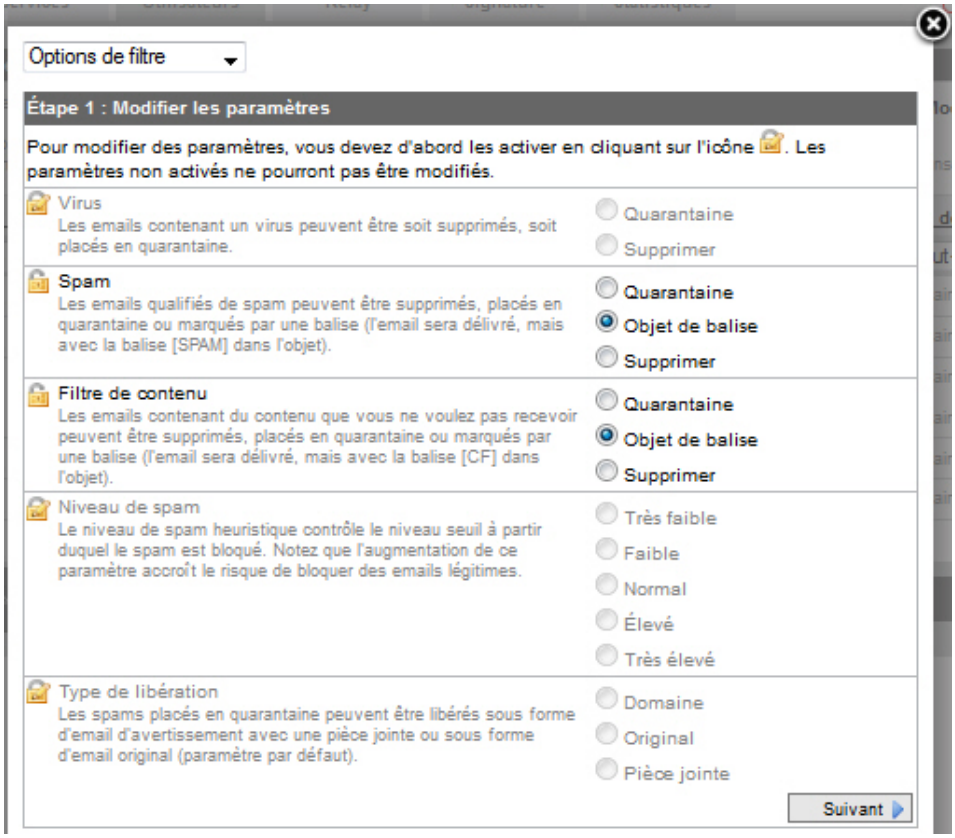


Pour supprimer tous les filtres et afficher la totalité de la liste des utilisateurs, cliquez sur le bouton **Réinitialiser les filtres** .

3. **Enfin, effectuez les modifications des paramètres utilisateurs** :

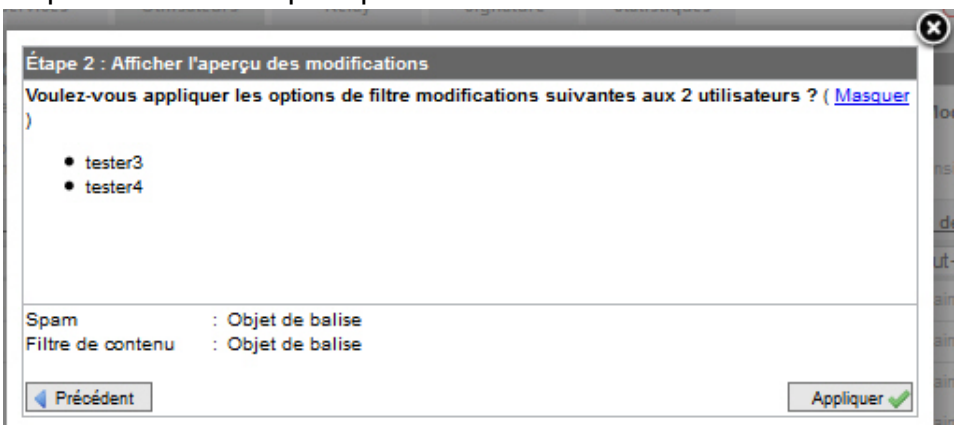
   Si vous souhaitez seulement supprimer les utilisateurs sélectionnés, cliquez sur **Supprimer la sélection** puis appuyez sur **OK** pour confirmer l'action.

   Cliquez sur le bouton **Modifier la sélection** pour démarrer la modification des services pour les utilisateurs sélectionnés. Vous pouvez cliquer directement sur **Modifier tout** si les modifications doivent s'appliquer à tous les utilisateurs de la liste.



4. Cliquez sur les icônes **Modifier** dans la première colonne de la feuille des paramètres et sélectionnez l'option que vous souhaitez activer pour les utilisateurs sélectionnés.

5. Cliquez sur **Suivant** pour passer en revue les modifications.



6. Vous pouvez cliquer sur **Afficher** ou sur **Masquer** pour afficher ou masquer la liste des utilisateurs sélectionnés dans la fenêtre d'aperçu.

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

   Les modifications effectuées seront mises à jour dans la vue **Utilisateurs**.

Aperçu des paramètres disponibles en Mode avancé

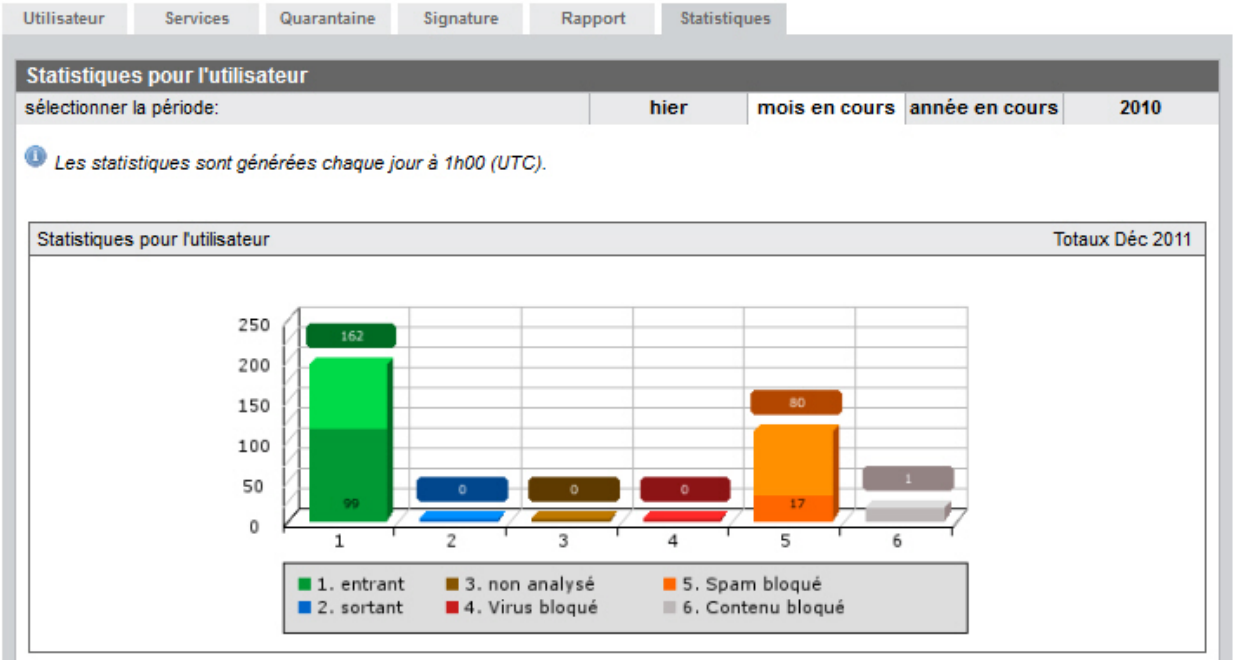
Groupes de paramètres	Paramètres	Options
Généralités	(Voir 3.3 Ajout de nouveaux utilisateurs à un domaine - page 12)	
	Actif	Oui / Non
	Administrateur	Oui / Non
	Livraison	Livraison SMTP (+ adresse IP ou hôte) Transfert de courrier (+ adresse email)
Services	(Voir 3.3 Ajout de nouveaux utilisateurs à un domaine - page 12)	
	Scan Antivirus	Activé / Désactivé
	Filtre antispam	Activé / Désactivé
	Filtre de contenu	Activé / Désactivé
Options de filtre	(Voir 4.1 Configuration des filtres d'emails - page 23)	
	Virus	Quarantaine / Supprimer
	Spam	Quarantaine Balise objet Supprimer

Groupes de paramètres	Paramètres	Options
	Filtre de contenu	Quarantaine Balise objet Supprimer
	Niveau de spam	Très faible Faible Normal Élevé Très élevé
	Type de libération	Domaine Original Pièce jointe
Liste noire / Liste blanche	(Voir 4.1.2 Ajustement des réglages des filtres - page 25)	
	Expéditeurs	Ajouter / Supprimer des entrées (+ adresse email)
	Domaines	Ajouter / Supprimer des entrées (+ domaines)
	Hôtes	Ajouter / Supprimer des entrées (+ hôtes)
Rapport général	(Voir 4.2 Définition des notifications de virus et de spam - page 29)	
	Notification de virus	Activé / Désactivé
	Rapport de quarantaine	Activé / Désactivé
	Langue	Anglais / Allemand
	Destinataire	Utiliser l'adresse email de chaque utilisateur Utiliser une adresse générale pour tous les utilisateurs (+ adresse email)
	Heure du rapport	l'heure
Rapport de contenu	(Voir 4.2 Définition des notifications de virus et de spam - page 29)	
	Contenu de rapport	100 derniers rapports 500 derniers rapports 100 derniers éléments 500 derniers éléments
	Inscrit sur liste noire	Afficher / Masquer
	Spam évident	Afficher / Masquer

Groupes de paramètres	Paramètres	Options
	Jeu de caractères	Aucun Russe Chinois Les deux
	Rapport vide	Activé / Désactivé

6. Statistiques

AMES crée des statistiques concernant les emails analysés, les virus interceptés, les spams et les contenus filtrés, **par domaine** et **par utilisateur**. Cliquez sur l'onglet **Statistiques** pour les vérifier.



Les informations sur les emails traités se divisent comme suit :

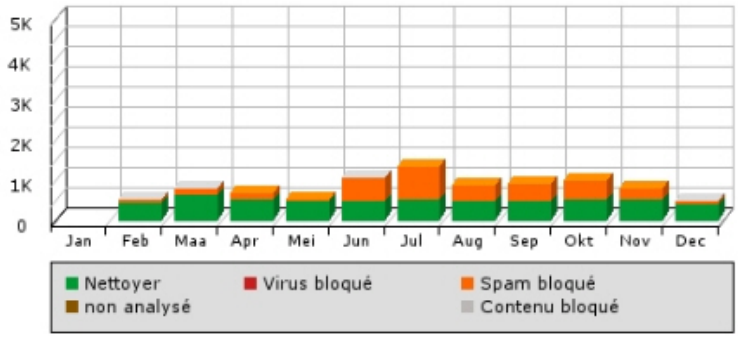
- **entrant** (vert) - quantité d'emails entrants ; le segment vert foncé représente les emails entrants pour lesquels le greylisting n'a **pas** été appliqué. Le greylisting s'applique uniquement aux utilisateurs catch-all. Voir « Liste grise » - page 17.
- **sortant** (bleu) - quantité d'emails sortants si le service relais est activé.
  Voir 2.4 Analyse des emails sortants - page 9.
- **non analysé** (marron) - quantité d'emails non analysés en raison de filtres désactivés.
- **Virus bloqué** (rouge) - quantité d'emails interceptés par le filtre à virus.
- **Spam bloqué** (orange) - quantité d'emails interceptés par le filtre à spams, y compris les éléments mis sur liste noire ; le segment orange foncé représente les emails archivés dans la quarantaine de spam.
- **Contenu bloqué** (gris) - quantité d'emails interceptés par le filtre de contenus.

> **Remarque**
> Les statistiques sont générées chaque jour à 1h00 (UTC).

Vous pouvez modifier la plage de temps des statistiques, avec le menu **sélectionner la période** : **hier**, **mois en cours**, **mois dernier**, **année en cours** ou année précédente.

Si vous sélectionnez par exemple le mois en cours, **les statistiques quotidiennes** sont également disponibles pour l'utilisateur ou le domaine sélectionné. De même, si vous sélectionnez une année, vous pouvez voir les **statistiques mensuelles** pour un utilisateur ou un domaine.

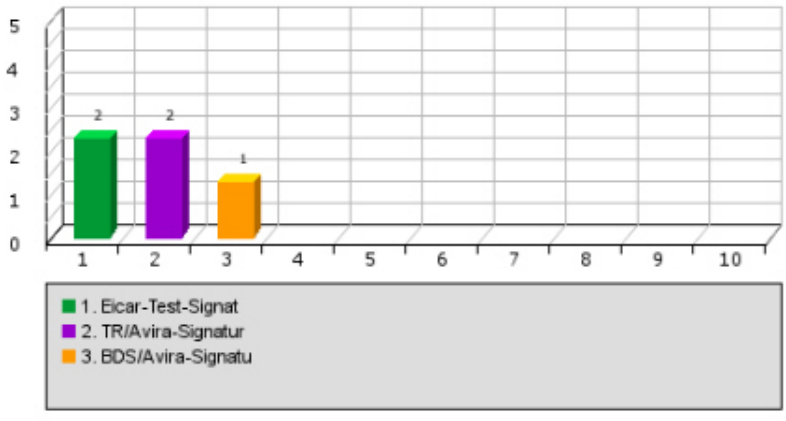
Statistiques pour l'utilisateur — Mensuellement 2011



date	dans	hors	taille	Virus		Spam		Contenu	
Fév 2011	225	0	15,10 MB	0	0,00%	106	47,11%	1	1%
Mar 2011	476	0	12,73 MB	5	1,05%	150	31,51%	3	1%
Avr 2011	362	0	7,46 MB	0	0,00%	154	42,54%	0	0%
Mai 2011	228	0	7,71 MB	0	0,00%	39	17,11%	0	0%
Juin 2011	763	0	2,25 MB	0	0,00%	576	75,49%	1	0%
Juil 2011	1.038	0	53,27 MB	0	0,00%	835	80,44%	0	0%
Août 2011	547	0	7,70 MB	0	0,00%	366	66,91%	0	0%
Sept 2011	599	0	4,61 MB	0	0,00%	414	69,12%	0	0%
Oct 2011	680	0	21,43 MB	0	0,00%	465	68,38%	0	0%
Nov 2011	483	0	4,37 MB	0	0,00%	280	57,97%	0	0%
Déc 2011	*162*	*0*	*4,57 MB*	0	0,00%	80	49,38%	1	1%
Total:	5.563	0	141,22 MB	5	0,09 %	3.465	62,29 %	6	0,11 %
Moyen:	506	0	12,84 MB	0	0,09 %	315	62,29 %	1	0,11 %

Vous pouvez aussi contrôler le rapport sur le **Top 10 des virus** interceptés par AMES au cours de la période sélectionnée.

Top 10 virus — Totaux 2011



D’autres statistiques indiquent le **Top 25 des expéditeurs** et le **Top 25 des destinataires** des emails durant la période sélectionnée.

Top 25 expéditeurs		2011
	expéditeur	Emails
1	demo@yahoo.com	3
2	demo@web.de	3
3	test@domain.com	2
4	test@domain.demo	1
5	test@domain.de	1
6	demo@domain.de	1
7	tester@domain.demo	1

Top 25 destinataires		2011
	destinataire	Emails
1	tester.demo@domain.demo	3.011

7. Support

Service de support

Toutes les informations sur notre service de support complet sont disponibles sur notre site web http://www.avira.com.

FAQ

Lisez également la section FAQ de notre site web.
Vos questions ont peut-être déjà été posées par d'autres utilisateurs et résolues dans cette section.

Veuillez contacter votre partenaire Avira – il vous aidera volontiers pour toute question relative aux produits Avira.

Contact

Adresse

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Allemagne

Internet

Vous trouverez d'autres informations sur nous et nos produits à l'adresse suivante :
http://www.avira.com

Edition du 1er trimestre 2012.

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
L'Allemagne

Téléphone: +49 7542-500 0
Fax: +49 7542-500 3000
Internet: www.avira.com