Control Panel - Manuel de l'administrateur

Table des matières

Informations générales

À propos du manuel

Ce manuel s'adresse aux administrateurs du Control Panel. Il contient des informations sur son utilisation et sur les tâches administratives.

Les droits administratifs sont répartis en deux catégories :

- Administrateur côté client : responsable d'un domaine principal, tous les domaines alias et adresses e-mail correspondants.
- Administrateur côté partenaire : responsable de plusieurs clients. Chaque client correspond à un domaine principal, à tous les domaines alias et adresses courriel correspondants.

REMARQUE :

Les modules et fonctions auxquels un utilisateur a accès dépendent de ses droits. Il est donc possible que certains des modules et fonctions décrits ne soient pas disponibles pour un utilisateur.

Ce manuel fournit dans un premier temps les informations de base suivantes sur le Control Panel : Le Control Panel est l'interface utilisateur permettant d'utiliser et de configurer nos services (voir Introduction à la page 8) et est pris en charge par différents navigateurs (voir Conditions à la page 9).

Le Control Panel est mis à jour en permanence afin d'introduire de nouvelles fonctions et améliorations. Le numéro de version actuel peut être consulté dans le Control Panel (voir Accéder au numéro de version à la page 9). Les modifications d'une version sont résumées dans les informations sur la version (voir Informations sur la version à la page 9). En outre, les utilisateurs peuvent contacter notre soutien technique via le Control Panel (voir Faire une demande d' assistance par chat).

De plus, ce manuel explique les premières étapes du Control Panel : Pour pouvoir accéder au Control Panel, les utilisateurs doivent d'abord se connecter (voir Se connecter à la page 10). Chaque utilisateur dispose de ses propres paramètres d'utilisateur et peut les personnaliser (voir

Paramètres des utilisateurs à la page 20). En outre, les administrateurs peuvent gérer les autorisations des utilisateurs (voir Gestion des droits dans le Control Panel à la page 48).

La suite du manuel décrit plus en détails les différents modules du Control Panel :

- **Tableau de bord** (voir À propos du tableau de bord)
- **Email Live Tracking** (voir Email Live Tracking à la page 59)
- **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100)
- **Rapports & conformité** (voir Rapports & conformité à la page 160)
- **Web Filter** (voir Télécharger le Web Filter)
- **Paramètres client** (voir Paramètres des clients à la page 213)
- **Sauvegarde** (voir Possibilités de sauvegarde)
- **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312)
- **Security Awareness Service** (voir À propos de Security Awareness Service)
- **Paramètres de sécurité** (voir Paramètres de sécurité)
- **Personnalisation** (voir Personnalisation du Control Panel à la page 608)

Il présente également les motifs de catégorisation à partir desquels les courriels sont attribuées à une catégorie dans le Control Panel (voir Raisons de catégorisation à la page 627).

Présentation du Control Panel

Introduction

Le Control Panel est l'interface utilisateur permettant d'utiliser et de configurer nos services. La fonction principale du Control Panel est la surveillance et la gestion des courriels.

Le Control Panel aide les utilisateurs à gérer les courriels qu'ils reçoivent et à évaluer leur trafic de courriels. Par exemple, les utilisateurs peuvent signaler des courriels comme spam et envoyer des courriels signalés comme spam. De plus, les utilisateurs peuvent interdire ou autoriser des expéditeurs (voir Actions sur les courriels à la page 89).

Le Control Panel a été développé en responsive design en tant qu'applicable web et peut être utilisé à la fois sur des appareils mobiles ou des ordinateurs de bureau.

Conditions

Le Control Panel est pris en charge par les navigateurs suivants :

- Google Chrome à partir de la version 55
- Mozilla Firefox à partir de la version 50
- Microsoft Edge à partir de la version 38
- Apple Safari à partir de la version 9

IMPORTANT :

Le mode Incognito des navigateurs cités n'est pas pris en charge.

Informations sur la version

Le Control Panel est mis à jour en permanence afin d'introduire de nouvelles fonctions et améliorations. Un numéro de version est attribué à chaque version (voir Accéder au numéro de version à la page 9). Les extensions et améliorations d'une version sont décrites dans les informations sur la version. Les informations sur la version actuelle sont disponibles ici. En outre, les informations sur la version sont liées au numéro de version dans le Control Panel.

Accéder au numéro de version

Vous pouvez accéder au numéro de la version actuelle du Control Panel dans le Control Panel. Les informations sur la version sont également reliées sous le numéro de version (voir Informations sur la version à la page 9).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez dans le coin supérieur droit de la fenêtre sur  à côté des Paramètres des utilisateurs.

Le numéro de la version actuelle apparaît en bas à droite dans le Control Panel. Sous le numéro de version se trouve un lien vers les informations sur la version.

3. Facultatif : Si vous souhaitez ouvrir les informations sur la version, cliquez sur le lien sous le numéro de version.

Les informations sur la version s'ouvrent.

Le numéro de version a été accédé.

Premiers pas dans le Control Panel

Se connecter

Votre administrateur a ajouté votre boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220).

REMARQUE :

Les administrateurs peuvent désactiver les boîtes aux lettres des utilisateurs dans le Control Panel (voir Activer ou désactiver une boîte aux lettres à la page 242). Les utilisateurs dont les boîtes aux lettres sont désactivées ne peuvent pas se connecter au Control Panel.

Pour accéder au Control Panel, vous devez vous connecter au Control Panel.

REMARQUE :

Pour des raisons de sécurité, un utilisateur est averti par courriel dès que plusieurs tentatives de connexion consécutives ont échoué pour son compte. La première notification est envoyée après 5 tentatives de connexion échouées. Une autre notification sera envoyée après 8 tentatives de connexion échouées et l'accès sera alors bloqué pendant 24 heures. Après chaque nouvelle tentative de connexion échouée, une nouvelle notification sera envoyée et l'accès sera à nouveau bloqué pendant 24 heures.

1. Saisissez l'URL du site Web du Control Panel dans votre navigateur pour vous connecter au Control Panel.

➔ La page de connexion apparaît.

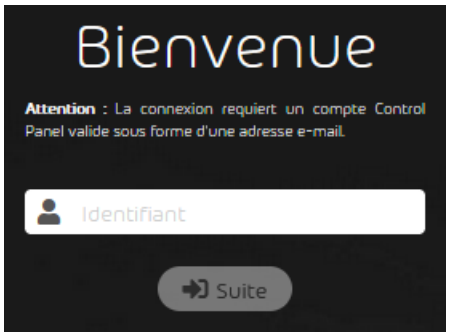


Illustration 1 : Connexion au Control Panel

2. Saisissez votre nom d'utilisateur dans le champ **Identifiant**.

> **REMARQUE :**
>
> Saisissez votre adresse courriel personnelle comme nom d'utilisateur. Après votre inscription, votre partenaire ou le support vous enverra vos données d'accès.

3. Cliquez sur **Suite**.

> **REMARQUE :**
>
> Si vous avez oublié votre mot de passe et que votre boîte aux lettres dans le Control Panel n'est pas synchronisée avec un service d'annuaire via LDAP , vous pouvez réinitialiser votre mot de passe (voir Réinitialiser le mot de passe à la page 17).

4. Effectuez les étapes suivantes si votre mot de passe est géré dans le Control Panel ou si vous vous connectez au Control Panel avec vos identifiants d'un service d'annuaire via LDAP.

   a) Saisissez votre mot de passe dans le champ **Mot de passe**.

Illustration 2 : Saisir le mot de passe

   b) Cliquez sur **Se connecter**.

Si l'authentification multifacteur n'est pas configurée pour le compte, le Control Panel s'ouvre. Lors de la première connexion au Control Panel, une fenêtre pour la sélection d'un fuseau horaire, d'une langue, d'un format de date et d'heure apparaît.

Si la connexion à un compte d'administrateur est effectuée et que l'authentification multifacteur est forcée pour les administrateurs (voir «#Forcer l'authentification multifacteur pour les administrateurs#» dans le manuel du Control Panel), l'administrateur doit configurer l'authentification multifacteur pour son compte (voir Configurer l'authentification multifacteur à partir de l'étape 7 à la page 27).

Si l'authentification multifacteur est configurée pour le compte (voir Configurer l'authentification multifacteur à la page 25), le champ **Mot de passe à usage unique** apparaît. Pour la connexion avec l'authentification multifacteur, des étapes supplémentaires sont nécessaires.

c) Si l'authentification multifacteur est configurée pour votre compte, ouvrez votre application Authenticator sur votre appareil mobile.

d) Saisissez le mot de passe unique actuel de l'application Authenticator dans le champ **Mot de passe à usage unique**.

Illustration 3 : Saisir un mot de passe unique

e) Cliquez sur **Se connecter**.

> **REMARQUE :**
>
> En cas de problème avec l'authentification multifacteur, l'administrateur peut réinitialiser l'authentification multifacteur du compte (voir Élimination des erreurs : Problèmes avec l' authentification multifacteur à la page 19 et « Réinitialiser l'authentification multifacteur » dans le manuel du Control Panel).

Le Control Panel s'ouvre. Si le partenaire a publié un contrat de licence d'utilisateur final et un contrat de traitement des données, les contrats apparaîtront. Lors de la première

connexion au Control Panel, une fenêtre pour la sélection d'un fuseau horaire, d'une langue, d'un format de date et d'heure apparaît.

5. Si vous êtes invité à définir un mot de passe d'urgence, saisissez un mot de passe dans le champ **Mot de passe d'urgence**. Ce mot de passe vous permet de vous connecter à notre système de messagerie Web en cas de panne du serveur mail de votre organisation. Après avoir défini le mot de passe d'urgence pour la première fois, vous pouvez le modifier dans vos paramètres utilisateur (voir Modifier le mot de passe d'urgence à la page 24).

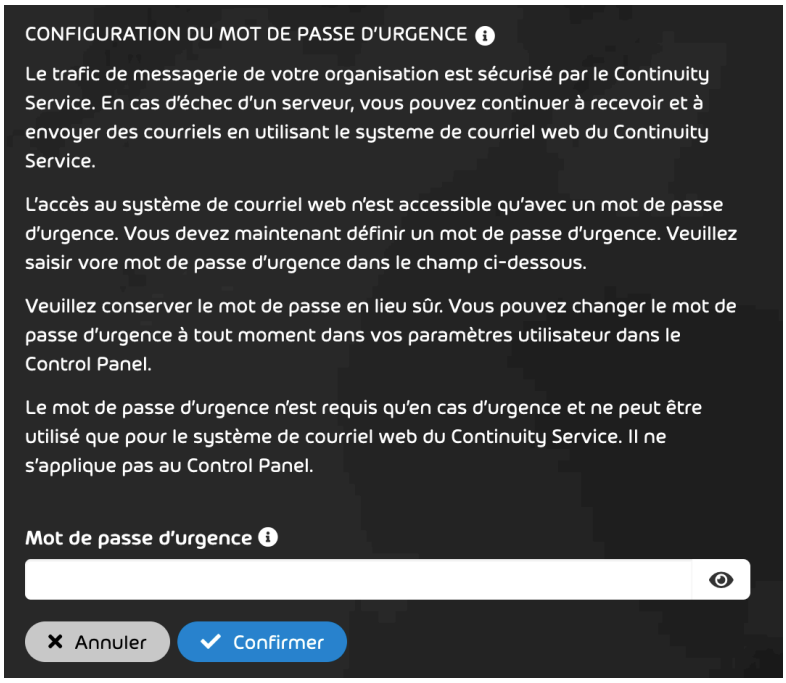


Illustration 4 : Définir le mot de passe d'urgence

6. **IMPORTANT :**

Les partenaires peuvent publier un contrat de licence d'utilisateur final et un contrat de traitement des données dans le Control Panel (voir « Conditions générales » dans le manuel du Control Panel). Chaque utilisateur doit accepter le contrat de licence d'utilisateur final afin de pouvoir accéder au Control Panel.

Si un contrat de licence d'utilisateur final et un contrat de traitement des données apparaissent, cela signifie que vous acceptez les conditions contractuelles.

a) Cochez la case **J'accepte les conditions du contrat de licence d'utilisateur final.**

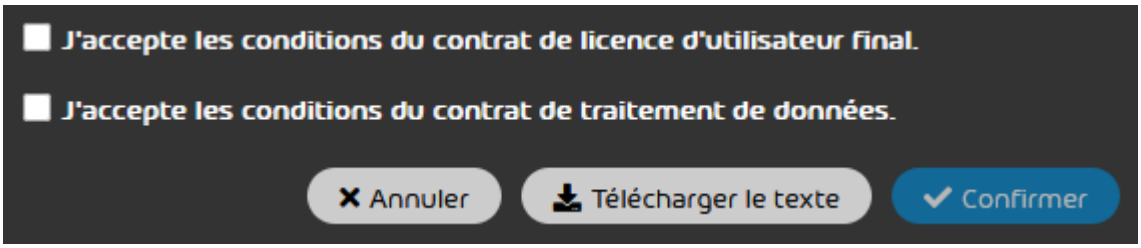


Illustration 5 : Accepter le contrat de licence d' utilisateur final

b) **IMPORTANT :**

Les contrats ne réapparaîtront pas dans le Control Panel après que l'utilisateur a donné son accord.

Facultatif : Si vous souhaitez enregistrer le texte des contrats, cliquez sur **Télécharger le texte**.

- Les contrats sont exportés sous forme de fichier .txt et rendus disponibles au téléchargement.

c) Facultatif : Si vous avez téléchargé le texte des contrats, enregistrez le fichier .txt sur votre système de fichiers.

d) Cliquez sur **Confirmer**.

- Les conditions contractuelles sont acceptées.

7. Si vous vous connectez au Control Panel pour la première fois, sélectionnez un fuseau horaire, une langue, un format de date et d'heure à partir des menus déroulants et cliquez sur **Confirmer**.

Illustration 6 : Sélectionner les paramètres

REMARQUE :

Pour de plus amples informations sur les paramètres, voir Modifier le fuseau horaire et la langue à la page 34. Vous pouvez modifier les paramètres à tout moment dans vos paramètres utilisateur.

La connexion au Control Panel a été établie.

REMARQUE :

Vous serez automatiquement déconnecté du Control Panel après 24#heures d'inactivité, si vous ne vous êtes pas déconnecté vous-même avant.

Réinitialiser le mot de passe

Votre compte n'est pas synchronisé via LDAP .

> **REMARQUE :**
>
> Si votre compte est synchronisé via LDAP , vous ne pouvez pas réinitialiser votre mot de passe vous-même. Pour réinitialiser votre mot de passe, contactez votre administrateur.

Si vous avez oublié le mot de passe de votre Control Panel, vous pouvez le réinitialiser.

1. Ouvrez la page de connexion du Control Panel.
2. Saisissez votre adresse courriel.
3. Cliquez sur **Réinitialiser le mot de passe ?**.

Illustration 7 : Réinitialiser le mot de passe

4. Cliquez sur **Envoyer**.

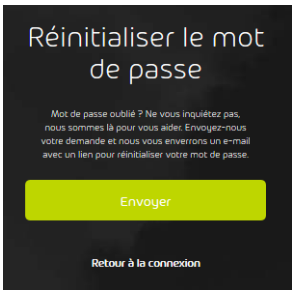


Illustration 8 : Confirmer la réinitialisation du mot de passe

- Vous recevrez un courriel avec un lien pour réinitialiser votre mot de passe.

> **REMARQUE :**
>
> Le lien est valable pendant une heure.

5. Ouvrez le courriel et cliquez sur le lien.

- Une fenêtre avec le formulaire de connexion au Control Panel s'ouvre.

6.

> **IMPORTANT :**
>
> Pour des raisons de sécurité, le nouveau mot de passe ne doit pas correspondre au mot de passe précédent.

Entrez le nouveau mot de passe et répétez-le.

7. Cliquez sur **Envoyer**.

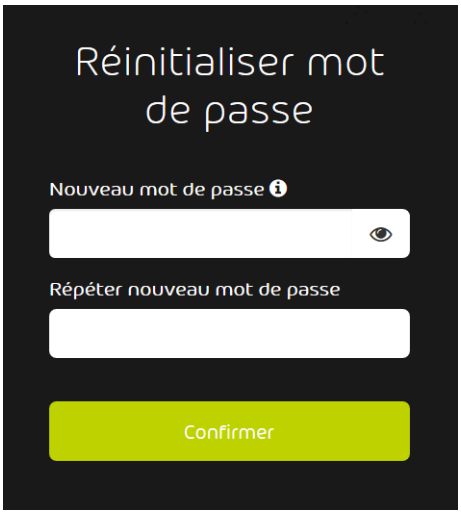


Illustration 9 : Confirmer le nouveau mot de passe

Le mot de passe a été modifié. Vous pouvez maintenant vous connecter au Control Panel avec le nouveau mot de passe.

- Si le lien pour réinitialiser votre mot de passe a expiré, cliquez à nouveau sur **Envoyer**. Vous recevrez un nouveau lien.

Élimination des erreurs : Problèmes avec l'authentification multifacteur

Problème

L'authentification multifacteur est configurée pour votre compte de Control Panel (voir Configurer l'authentification multifacteur à la page 25). Vous ne pouvez pas vous connecter au Control Panel.

Raison

Vous ne pouvez pas récupérer le mot de passe unique nécessaire pour la connexion au Control Panel via l'application Authenticator sur votre appareil mobile, car vous n'avez plus accès à l'application ou à l'appareil mobile.

Solution

Contactez votre administrateur.

- L'administrateur réinitialise l'authentification multifacteur pour le compte (voir le chapitre «#Réinitialiser l'authentification multifacteur#» dans le manuel du Control Panel). La configuration de l'authentification multifacteur est supprimé pour le compte. Désormais, seul le mot de passe du Control Panel est nécessaire pour se connecter au Control Panel. Il est possible de reconfigurer l'authentification multifacteur (voir Configurer l'authentification multifacteur à la page 25).

Paramètres des utilisateurs

Dans les paramètres des utilisateurs, les utilisateurs peuvent gérer leurs paramètres personnels. Les paramètres des utilisateurs sont accessibles via l'icône en forme de roue dentée en haut à droite dans le Control Panel (voir Ouvrir les paramètres utilisateur à la page 21). Les paramètres des utilisateurs comprennent les paramètres généraux concernant le mot de passe, le mot de passe d'urgence pour le système de messagerie Web du Continuity Service (voir À propos du Continuity Service à la page 603), l'authentification multifacteur, les données de base, le fuseau horaire et la langue d'un utilisateur. En outre, les clés d'API, les notes d'absence et les paramètres pour les rapports de quarantaine peuvent être gérés.

Les utilisateurs dont les mots de passe sont gérés dans le Control Panel peuvent modifier leur mot de passe (voir Modifier le mot de passe à la page 22). Si l'administrateur l'autorise (voir « Activer l'authentification multifacteur » dans le manuel du Control Panel), les utilisateurs dont les mots de passe sont gérés dans le Control Panel ou dans un service d'annuaire via LDAP peuvent configurer l'authentification multifacteur pour leur compte (voir Configurer l'authentification multifacteur à la page 25). Cela permet d'améliorer la sécurité lors de la connexion au Control Panel. S'ils le souhaitent, les utilisateurs peuvent également désactiver l'authentification multifacteur pour leur compte (voir Désactiver l'authentification multifacteur à la page 30).

Les utilisateurs dont les boîtes aux lettres dans le Control Panel ne sont pas synchronisées avec un service d'annuaire via LDAP peuvent éditer leurs données de base (voir Éditer les données de base à la page 36). Pour les utilisateurs des boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la

page 218), les données de base sont synchronisées avec le service d'annuaire. Les utilisateurs de ces boîtes aux lettres peuvent consulter leurs données de base, mais pas les modifier.

Chaque utilisateur peut choisir un fuseau horaire, une langue, un format de date et d'heure (voir Modifier le fuseau horaire et la langue à la page 34). Les paramètres s'appliquent à l'affichage dans le Control Panel et aux courriels automatiques du Control Panel.

Les administrateurs et les utilisateurs avec le rôle **Service Desk** peuvent créer des clés d'API qui permettent aux applications d'accéder au Control Panel via l'API (voir Créer un jeton API à la page 38). Les jetons API peuvent également être supprimés du Control Panel (voir Supprimer un jeton API à la page 41), ce qui les rend invalides.

En outre, les utilisateurs peuvent créer des notes d'absence (voir Créer une note d' absence à la page 42) pour informer automatiquement les expéditeurs de leurs courriels entrants de leur absence. Si l'administrateur l'autorise, les utilisateurs peuvent également modifier les paramètres de leurs propres rapports de quarantaine (voir Configurer les rapports de quarantaine à la page 43).

Ouvrir les paramètres utilisateur

Vous pouvez ouvrir vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20) dans le Control Panel. Dans les paramètres utilisateur, vous pouvez gérer les paramètres généraux, tels que votre fuseau horaire et votre langue (voir Modifier le fuseau horaire et la langue à la page 34) ainsi que des jetons API (voir Créer un jeton API à la page 38 et Supprimer un jeton API à la page 41), les notes d'absence (voir Créer une note d' absence à la page 42) et les paramètres de vos rapports de quarantaine (voir Configurer les rapports de quarantaine à la page 43).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur  en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 10 : Paramètres des utilisateurs

Les paramètres utilisateur ont été ouverts.

Paramètres

Modifier le mot de passe

Si votre boîte aux lettres n'est pas synchronisée avec un service d'annuaire via LDAP, vous pouvez modifier votre mot de passe du Control Panel dans vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20).

REMARQUE :

Les utilisateurs de boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218) peuvent se connecter au Control Panel avec leurs identifiants du service d'annuaire. Par conséquent, ces utilisateurs ne peuvent pas modifier leurs mots de passe dans le Control Panel. Les paramètres de mot de passe sont masqués pour ces utilisateurs.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

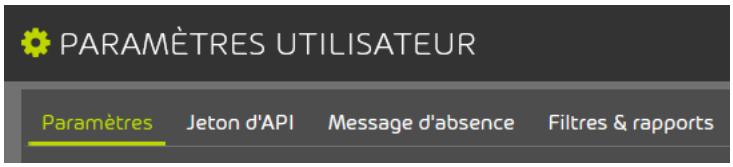


Illustration 11 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.

4. Saisissez votre mot de passe actuel dans le champ **Ancien mot de passe**.

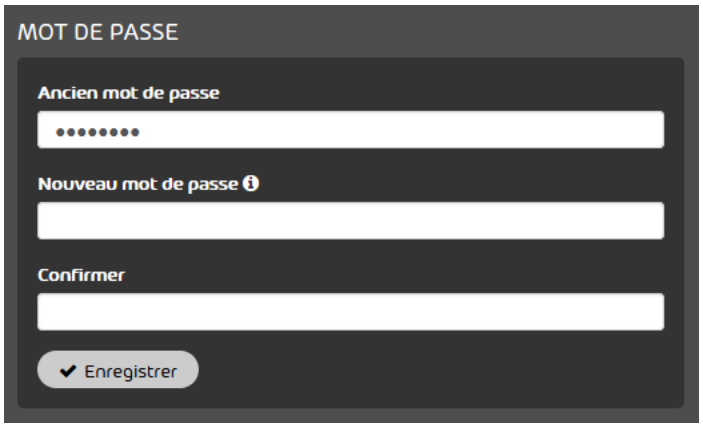


Illustration 12 : Saisir l'ancien mot de passe

5. **IMPORTANT :**

   Les nouveaux mots de passe doivent contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. Les nouveaux mots de passe doivent également avoir une longueur minimale définie par un administrateur côté client ou côté partenaire. Dans tous les cas, les mots de passe doivent toutefois comporter au moins 8 caractères.

   IMPORTANT :

   Pour des raisons de sécurité, le nouveau mot de passe ne doit pas correspondre au mot de passe précédent.

   Saisissez votre nouveau mot de passe dans le champ **Nouveau mot de passe**.

6. Saisissez à nouveau le nouveau mot de passe dans le champ **Confirmer**.
7. Cliquez sur **Enregistrer**.

Le nouveau mot de passe est sauvegardé. Pour des raisons de sécurité, l'utilisateur est notifié par courriel de la modification du mot de passe.

Le mot de passe a été modifié.

Modifier le mot de passe d’ urgence

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur  en haut à droite dans le Control Panel.

➔ Les paramètres utilisateur apparaissent.

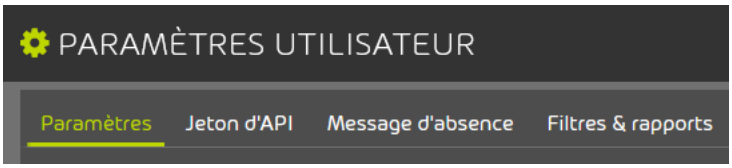


Illustration 13 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.
4. Saisissez votre nouveau mot de passe d'urgence dans le champ **Mot de passe d’ urgence**.

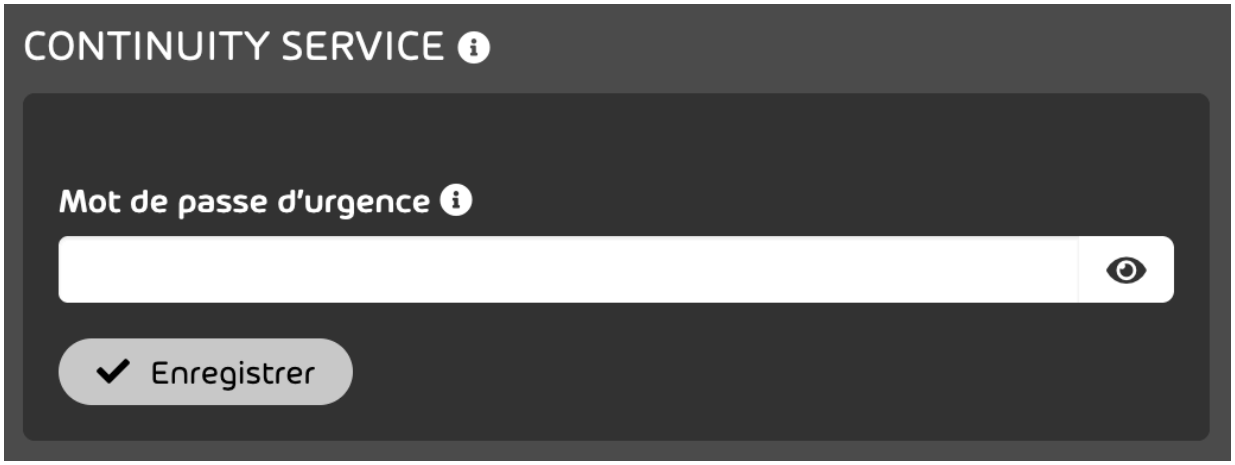


Illustration 14 : Modifier le mot de passe d’ urgence

5. Cliquez sur **Enregistrer**.

➔ Le nouveau mot de passe d'urgence est sauvegardé.

Le mot de passe d'urgence a été modifié.

Configurer l’ authentification multifacteur

Vos identifiants pour le Control Panel sont gérées dans le Control Panel ou dans un service d'annuaire via LDAP. Votre administrateur a activé l'authentification multifacteur pour les utilisateurs de votre domaine (voir « Activer l'authentification multifacteur » dans le manuel du Control Panel). Vous avez installé une application Authenticator TOTP (par ex. Microsoft Authenticator, Google Authenticator) sur votre appareil mobile.

Vous pouvez configurer l'authentification multifacteur pour votre compte du Control Panel. L'authentification multifacteur améliore la sécurité lors de la connexion au Control Panel. Nous recommandons en particulier aux administrateurs d'utiliser l'authentification multifacteur.

L'authentification multifacteur dans le Control Panel utilise la méthode TOTP. TOTP signifie « mots de passe uniques limités dans le temps ». Pour vous connecter au Control Panel avec l'authentification multifacteur, vous devez saisir, en plus du mot de passe du Control Panel, un mot de passe unique d'une application Authenticator (voir Se connecter à la page 10).

1. Connectez-vous au Control Panel.
2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

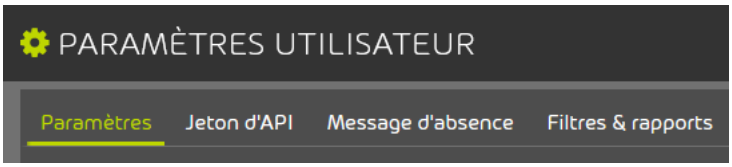


Illustration 15 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.

4. Actionnez le bouton **Activer l'authentification multifacteur** sous **Authentification multifacteur**.

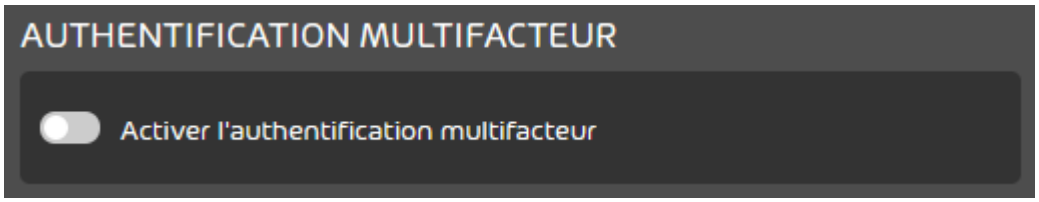


Illustration 16 : Activer l' authentification multifacteur

- Le bouton devient vert et une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

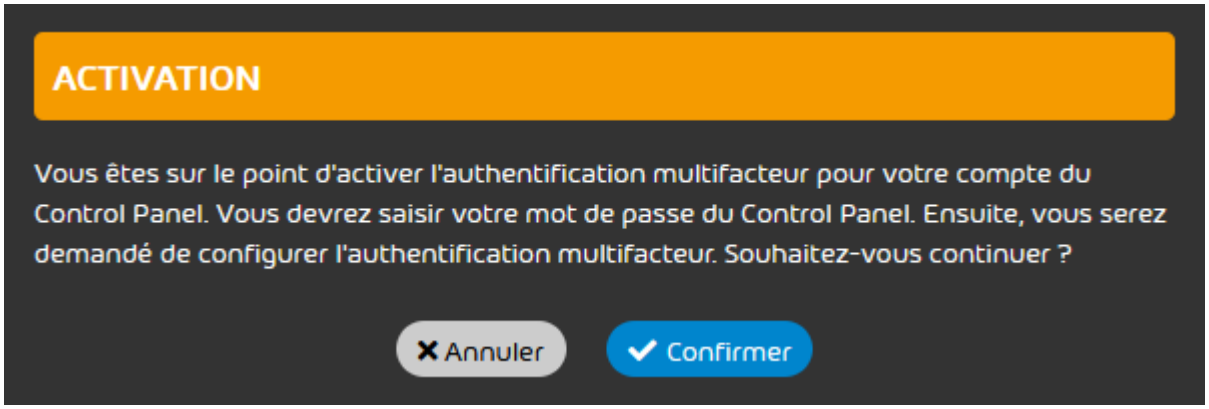


Illustration 17 : Confirmer

- La page **Configuration de l'authentification multifacteur** apparaît.

6. Saisissez votre mot de passe de Control Panel dans le champ de saisie.

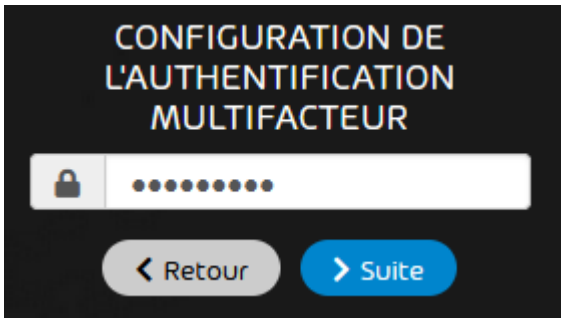


Illustration 18 : Saisir le mot de passe

7. Cliquez sur **Suite**.

Une page contenant des instructions sur la configuration de l'authentification multifacteur apparaît.

Illustration 19 : Configuration de l' authentification multifacteur

8. Ouvrez votre application Authenticator sur votre appareil mobile.

> **REMARQUE :**
>
> Certains navigateurs supportent les plug-ins Authenticator. Les utilisateurs qui ne disposent pas d'un appareil mobile peuvent utiliser un plug-in Authenticator dans le navigateur de leur PC au lieu d'une application Authenticator.

9. Ajoutez un nouveau compte à l'application Authenticator.

10.

> **IMPORTANT :**
>
> Un code QR ou une clé secrète est nécessaire pour configurer l'authentification multifacteur. Le code QR ne sera affiché dans le Control Panel qu'une seule fois. La clé secrète elle-aussi ne peut être affichée dans le Control Panel qu'une seule fois.
>
> Si l'authentification multifacteur est configurée pour une boîte aux lettres partagée, tous les propriétaires de la boîte aux lettres devront alors utiliser le même code QR ou la même clé secrète afin de configurer l'authentification multifacteur dans leur application Authenticator. C'est pourquoi la première personne à configurer l'authentification multifacteur pour la boîte aux lettres doit faire une capture d'écran du code QR ou enregistrer la clé secrète et la mettre à la disposition des autres propriétaires de la boîte aux lettres.

Facultatif : Si vous souhaitez configurer l'authentification multifacteur avec le code QR, procédez comme suit.

a) Si votre boîte aux lettres est une boîte aux lettres partagée, faites une capture d'écran du code QR à partir du Control Panel et conservez-la en lieu sûr.

b) Scannez le code QR à partir du Control Panel à l'aide de l'application Authenticator.

L'application Authenticator génère un nouveau mot de passe unique à six chiffres toutes les 30#secondes.

11. Facultatif : Si vous souhaitez configurer l'authentification multifacteur avec la clé secrète, procédez comme suit.

a) Cliquez sur **Afficher la clé secrète**.

➔ La clé secrète apparaît.

Illustration 20 : Clé secrète

b) Cliquez sur **Copier**.

➔ La clé secrète est copiée dans le presse-papiers.

c) Si votre boîte aux lettres est une boîte aux lettres partagée, enregistrez la clé secrète et conservez-la en lieu sûr.

d) Saisissez la clé secrète dans l'application Authenticator.

➔ L'application Authenticator génère un nouveau mot de passe unique à six chiffres toutes les 30#secondes.

12. Saisissez le mot de passe unique actuel de l'application Authenticator dans le masque de saisie du Control Panel.

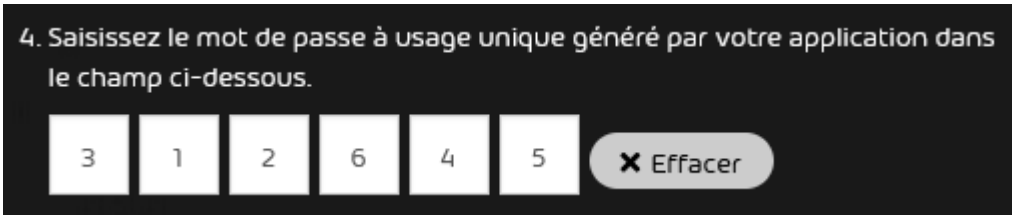


Illustration 21 : Saisir le mot de passe unique

13. Facultatif : Si vous souhaitez vider le masque de saisie pour saisir un autre mot de passe unique, cliquez sur **Effacer**.

➔ Le masque de saisie est vidé.

14. Cliquez sur **Confirmer**.

L'authentification multifacteur est configurée. L'authentification multifacteur sera désormais utilisée pour la connexion au Control Panel.

L'authentification multifacteur a été configurée.

Vous pouvez ensuite vous connecter au Control Panel à l'aide de l'authentification multifacteur (voir Se connecter à la page 10). Si vous ne souhaitez plus utiliser l'authentification multifacteur, vous pouvez la désactiver pour votre compte (voir Désactiver l'authentification multifacteur à la page 30). Si vous avez des problèmes avec l'authentification multifacteur, vous pouvez contacter votre administrateur (voir Élimination des erreurs : Problèmes avec l'authentification multifacteur à la page 19).

Désactiver l'authentification multifacteur

Vous avez configuré l'authentification multifacteur pour votre compte du Control Panel (voir Configurer l'authentification multifacteur à la page 25).

Si vous ne souhaitez plus utiliser l'authentification multifacteur, vous pouvez désactiver l'authentification multifacteur pour votre compte de Control Panel. L'authentification multifacteur améliore la sécurité lors de la connexion au Control Panel, car un mot de passe unique provenant d'une application Authenticator est nécessaire en plus du mot de passe du Control Panel.

REMARQUE :

Nous recommandons en particulier aux administrateurs d'utiliser l'authentification multifacteur.

1. Connectez-vous au Control Panel.
2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 22 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.
4. Actionnez le bouton **Activer l'authentification multifacteur** sous **Authentification multifacteur**.

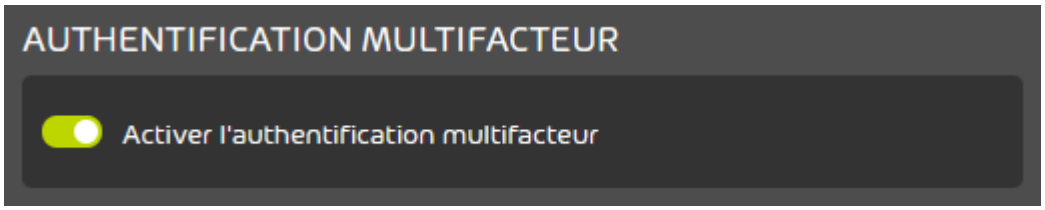


Illustration 23 : Désactiver l’ authentification multifacteur

- Le bouton devient gris et une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

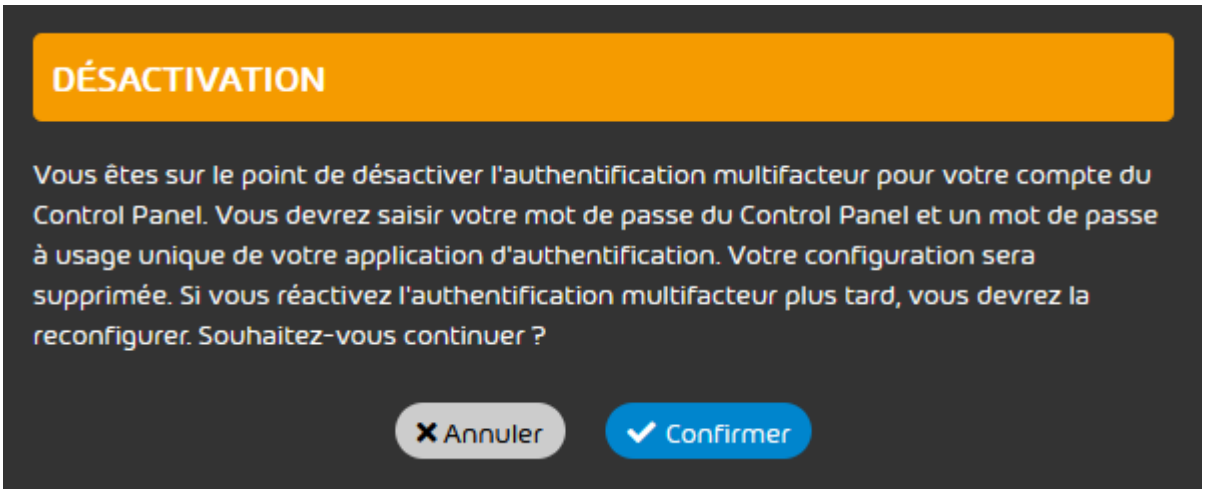


Illustration 24 : Confirmer

La page **Configuration de l'authentification multifacteur** apparaît.

6. Saisissez votre mot de passe du Control Panel dans le champ supérieur.

Illustration 25 : Saisir le mot de passe

7. Ouvrez votre application Authenticator sur votre appareil mobile.

8. Saisissez le mot de passe unique actuel de l'application Authenticator dans le champ inférieur.

Illustration 26 : Saisir un mot de passe unique

- Le bouton **Suite** est déverrouillé.

9. Cliquez sur **Suite**.

- L'authentification multifacteur est désactivée pour le compte. La configuration de l'authentification multifacteur est supprimée pour le compte. Un mot de passe unique provenant d'une application Authenticator n'est désormais plus nécessaire pour se connecter au Control Panel.

10. Facultatif : Supprimez le compte pour l'authentification multifacteur de votre application Authenticator.

L'authentification multifacteur a été désactivée pour le compte.

Vous pouvez ensuite vous connecter au Control Panel sans l'authentification multifacteur (voir Se connecter à la page 10). Si vous souhaitez réutiliser l'authentification multifacteur par la suite, vous pouvez reconfigurer l'authentification multifacteur (voir Configurer l' authentification multifacteur à la page 25).

Modifier le fuseau horaire et la langue

Vous pouvez modifier le fuseau horaire, la langue, le format de la date et le format de l'heure dans vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20). Ces paramètres s'appliquent à l'affichage dans le Control Panel et aux courriels automatiques du Control Panel.

REMARQUE :

Chaque utilisateur choisit un fuseau horaire, une langue, un format de date et d'heure lors de sa première connexion au Control Panel. Les utilisateurs peuvent modifier ces paramètres à tout moment dans les réglages des utilisateurs.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 27 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.

Les paramètres du fuseau horaire, de la langue, du format de la date et de l'heure sont affichés dans la section **Fuseau horaire et langue**.

Illustration 28 : Fuseau horaire et langue

4. Dans le menu déroulant **Fuseau horaire**, sélectionnez un fuseau horaire.

> **REMARQUE :**
>
> Le fuseau horaire détermine le format des chiffres dans le Control Panel et dans les courriels automatiques du Control Panel.

5. Dans le menu déroulant **Langue**, sélectionnez une langue.
6. Dans le menu déroulant **Format de date**, sélectionnez un format de date.

> **REMARQUE :**
>
> Le format de date détermine l'ordre dans lequel les données disponibles d'une date sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

7. Dans le menu déroulant **Format d'heure**, sélectionnez un format d'heure.

> **REMARQUE :**
>
> Le format d'heure détermine l'ordre dans lequel les données disponibles d'une heure sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

8. Cliquez sur **Enregistrer**.

Les modifications sont enregistrées.

Le fuseau horaire, la langue, le format de date et d'heure ont été modifiés.

Éditer les données de base

Sous **Paramètres utilisateur** (voir Paramètres des utilisateurs à la page 20) vous pouvez éditer les données de base de votre boîte aux lettres. Les données de base sont des informations sur le propriétaire d'une boîte aux lettres.

> **REMARQUE :**
>
> Les utilisateurs des boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218) ne peuvent pas éditer leurs données de base dans le Control Panel. Si des données de base sont enregistrées dans le service d'annuaire pour ces boîtes aux lettres, ces données sont affichées dans le Control Panel.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur  en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 29 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Paramètres**.

Dans la partie supérieure de la page, s'affiche la section **Données de base**.

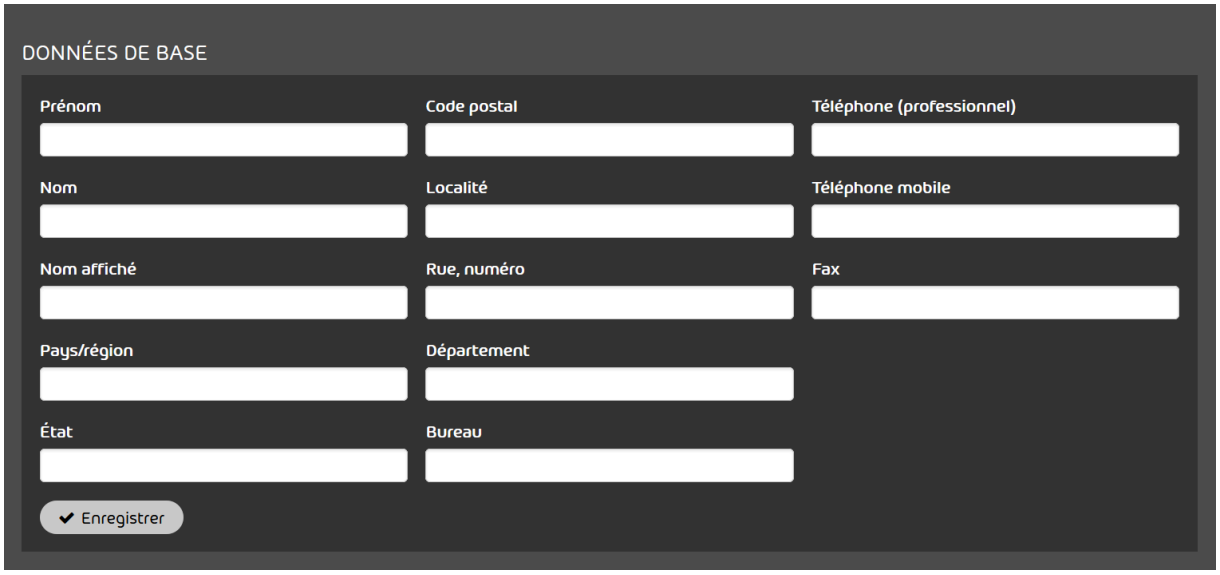


Illustration 30 : Données de base

4. **REMARQUE :**

   Tous les champs sont facultatifs.

   Saisissez vos données dans les champs. Les champs ont les significations suivantes :

   - **Prénom** : votre prénom
   - **Nom** : votre nom
   - **Nom affiché** : votre nom affiché dans le Control Panel
   - **Pays/région** : pays ou région où se trouve votre entreprise
   - **État** : land ou canton où se trouve votre entreprise
   - **Code postal** : code postal de votre entreprise
   - **Localité** : lieu où se trouve votre entreprise
   - **Rue, numéro** : rue et numéro où se trouve votre entreprise
   - **Département** : service dans lequel vous travaillez
   - **Bureau** : bureau où vous travaillez
   - **Téléphone (professionnel)** : votre numéro de téléphone professionnel
   - **Téléphone mobile** : votre numéro de téléphone mobile
   - **Fax** : votre numéro de fax

5. Cliquez sur **Enregistrer**.

Les modifications sont enregistrées.

Les données de base ont été éditées.

Créer un jeton API

Avec un jeton API, vous pouvez donner accès à l'API du Control Panel aux applications. Chaque application a besoin de son propre jeton. Dans vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20), vous pouvez créer un jeton API pour l'autorisation dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 31 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Jeton d'API**.
4. Cliquez sur **Créer jeton**.

Illustration 32 : Créer un jeton

D'autres paramètres apparaissent.

5. Dans le champ **Nom de l'application**, saisissez un nom pour l'application qui doit utiliser le jeton.

> **REMARQUE :**
>
> Dans le module **Audit 2.0**, les actions effectuées avec ce jeton sont désignées par le nom de l'utilisateur qui a créé le jeton.

Illustration 33 : Saisir le nom de l' application

6. Facultatif : Sous **Expire**, sélectionnez une date d'expiration pour le jeton.

> **REMARQUE :**
>
> **Jamais** est la valeur par défaut sélectionnée.

7.
> **PRUDENCE :**
>
> Pour des raisons de sécurité, le jeton n'est affiché qu'une seule fois. Si vous ne sauvegardez pas le jeton, il sera perdu. Sauvegarder le jeton directement.

Cliquez sur **Créer**.

Le jeton API est créé et affiché.

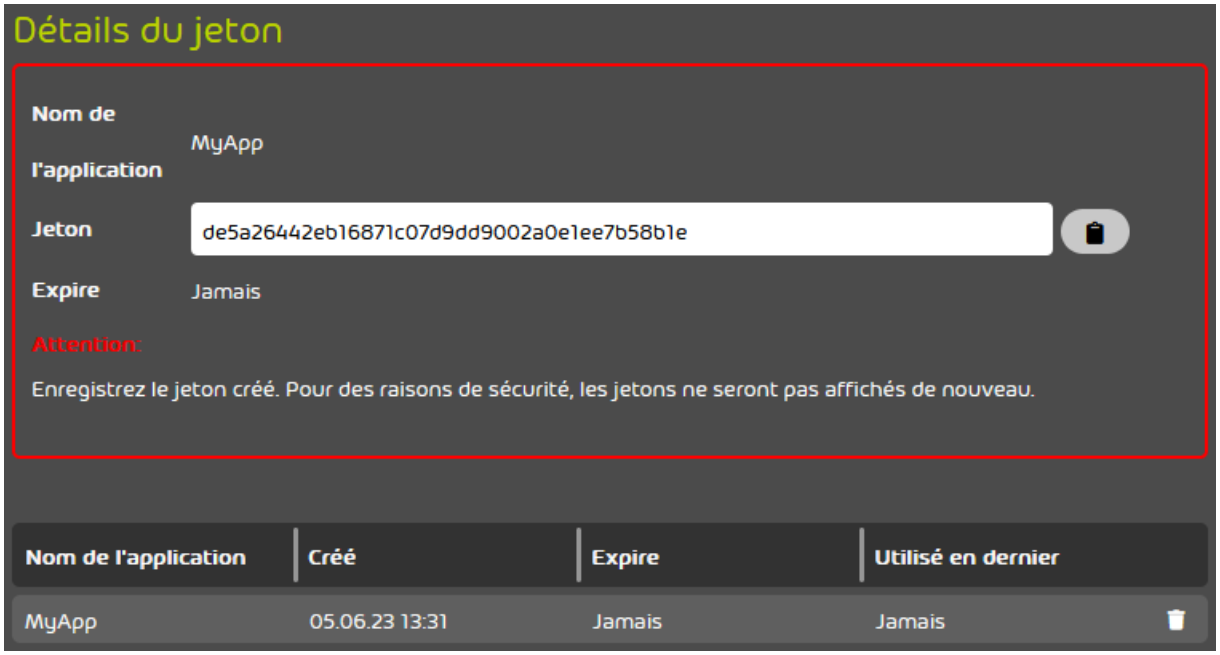


Illustration 34 : Jeton créé

Un jeton API a été créé.

Si vous n'avez plus besoin d'un jeton API, vous pouvez le supprimer du Control Panel (voir Supprimer un jeton API à la page 41).

Supprimer un jeton API

Vous avez créé un jeton API (voir Créer un jeton API à la page 38).

Si vous n'avez plus besoin d'un jeton API avant sa date d'expiration, vous pouvez le supprimer dans vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20) depuis le Control Panel. Cela rend le jeton API invalide. Le jeton API ne permet alors plus d'accéder à l'API du Control Panel.

1. Connectez-vous au Control Panel à l'aide des données d'accès de l'utilisateur qui a créé le jeton.

2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 35 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Jeton d'API**.
4. Dans la liste, sélectionnez le jeton que vous souhaitez supprimer.

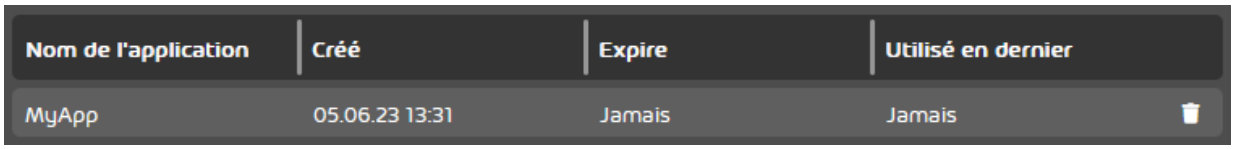


Illustration 36 : Sélectionner le jeton

5. Cliquez sur la croix à côté du jeton.

Le jeton est supprimé du système.

Un jeton API a été supprimé du système et rendu invalide.

Créer une note d'absence

Dans vos paramètres utilisateur, vous pouvez ajouter une note d'absence personnelle à votre compte de messagerie (voir Paramètres des utilisateurs à la page 20). Vous pouvez rédiger un texte individuel pour la note d'absence et activer ou désactiver la note d'absence à tout moment. Une fois que vous avez activé la note d'absence, tous les expéditeurs de vos courriels entrants reçoivent automatiquement un message concernant votre absence.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur en haut à droite dans le Control Panel.

Les paramètres utilisateur apparaissent.

Illustration 37 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Message d'absence**.
4. Dans le champ de texte libre, saisissez un texte pour la note d'absence.

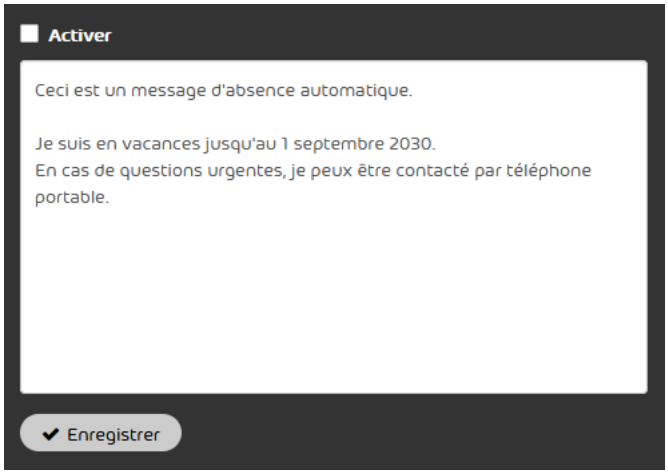


Illustration 38 : Saisir un texte

5. Cliquez sur **Enregistrer**.

Le texte de la note d'absence est enregistré.

6. Facultatif : Pour activer la note d'absence, cochez la case **Activer**.

La note d'absence est activée. Des courriels avec la note d'absence seront désormais automatiquement envoyés aux expéditeurs des courriels entrants.

Une note d'absence a été créée.

Configurer les rapports de quarantaine

Si votre administrateur le permet, vous pouvez, en tant qu'utilisateur, activer ou désactiver le filtre infomail pour votre propre boîte aux lettres et modifier les paramètres de vos rapports de

quarantaine. Vous pouvez modifier ces paramètres dans vos paramètres utilisateur (voir Paramètres des utilisateurs à la page 20).

Si le filtre infomail est activé, les courriels entrants de la catégorie **Infomail** seront, selon la configuration de l'administrateur, soit mis en quarantaine et repris dans vos rapports de quarantaine, soit marqués et vous seront directement envoyés. La catégorie **Infomail** comprend les courriels publicitaires, notamment les newsletters.

Vous pouvez modifier les heures de distribution de vos rapports de quarantaine. En outre, vous pouvez exclure de vos rapports de quarantaine les courriels dont les expéditeurs figurent sur votre propre liste des expéditeurs interdits ou sur la liste des expéditeurs interdits de votre domaine.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Cliquez sur  en haut à droite dans le Control Panel.

➔ Les paramètres utilisateur apparaissent.

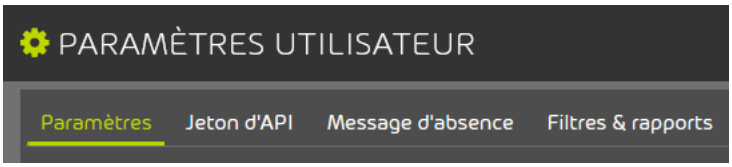


Illustration 39 : Paramètres des utilisateurs

3. Sélectionnez l'onglet **Filtres & rapports**.

➔ Les paramètres des rapports de quarantaine s'ouvrent. Les paramètres de l'administrateur sont prédéfinis.

4. **REMARQUE :**

   Les utilisateurs ne peuvent modifier les paramètres que si leur administrateur le permet.

   Actionnez le commutateur pour activer ou désactiver le filtre infomail.

Illustration 40 : Activer le filtre infomail

- Si le bouton est vert, cela signifie que le filtre infomail est activé et que les courriels classés comme **Infomail** sont soit mis en quarantaine et repris dans les rapports de quarantaine, soit marqués et directement distribués. L'administrateur décide de la manière dont les courriels sont traités.

5. Pour modifier les paramètres de vos rapports de quarantaine, utilisez le bouton **Définir vos propres moments de distribution**.

Illustration 41 : Définir vos propres moments de distribution

- Les paramètres des rapports de quarantaine sont activés.

REMARQUE :

Le module Quarantine Report est défini au niveau de la boîte aux lettres principale. Les rapports de quarantaine sont créés et délivrés pour chacune des boîtes aux lettres principales. Si des boîtes aux lettres alias sont associées à une boîte aux lettres principale, les courriels destinés aux boîtes aux lettres alias sont répertoriés dans un rapport de quarantaine avec les courriels destinés à la boîte aux lettres principale.

6.

IMPORTANT :

Ce paramètre ne peut être modifié que si les heures de distribution des rapports de quarantaine sont configurées.

Si vous souhaitez exclure des rapports de quarantaine les courriels provenant d'expéditeurs figurant sur votre liste des expéditeurs interdits ou sur la liste des expéditeurs interdits de votre domaine, actionnez le bouton **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine**.

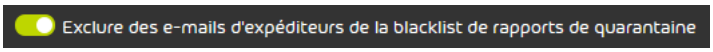


Illustration 42 : Exclure des courriels d'expéditeurs interdits de rapports de quarantaine

REMARQUE :

Si cette option est activée, les courriels provenant d'expéditeurs interdits (voir le chapitre « À propos des expéditeurs interdits et autorisés » dans le manue du Control Panel) par l'utilisateur ou le domaine ne sont pas mentionnés dans les rapports de quarantaine de l'utilisateur.

Si l'administrateur a choisi la mise en page **Inbox Manager avec l'aperçu du courriel et l'option d'exclusion** pour les rapports de quarantaine de ses utilisateurs (voir « Mises en page pour les rapports de quarantaine » dans le manuel du Control Panel), cette option sera activée et ne pourra pas être désactivée. Les rapports de quarantaine avec cette mise en page disposent du bouton **Ne jamais afficher l'expéditeur**. Ce bouton permet aux utilisateurs de mettre un expéditeur sur leur propre blacklist afin que les courriels de cet expéditeur n'apparaissent plus dans les futurs rapports de quarantaine. Les utilisateurs ne peuvent pas choisir eux-mêmes la mise en page de leurs rapports de quarantaine.

Le bouton devient vert. Les futurs rapports de quarantaine ne contiendront plus les courriels dont l'expéditeur figure sur la blacklist de la boîte aux lettres ou du domaine.

7. Si vous souhaitez désactiver les rapports de quarantaine pour votre boîte aux lettres, activez le bouton **Désactiver**.

Illustration 43 : Désactiver le Quarantine Report

Tous les jours et moments de distribution sont désactivés pour la boîte aux lettres. Aucun rapports de quarantaine n'est envoyé. Aucun autre paramètre n'est nécessaire.

8. Si les rapports de quarantaine pour votre boîte aux lettres restent activés, sélectionnez les jours où les rapports de quarantaine doivent être distribués. Sélectionnez au moins un jour.
   - Pour diffuser les rapports de quarantaine tous les jours, activez le bouton **Chaque jour**.
   - Pour recevoir les rapports de quarantaine quotidiennement du lundi au vendredi, activez le bouton **Les jours de la semaine**.
   - Cochez les cases des jours souhaités.

Illustration 44 : Sélectionner les jours

9. Sélectionnez les heures auxquelles les rapports de quarantaine doivent être distribués. Sélectionnez au moins une heure.

   - Pour diffuser les rapports de quarantaine toutes les heures, activez le bouton **Chaque heure**.
   - Cochez les cases des heures souhaitées.

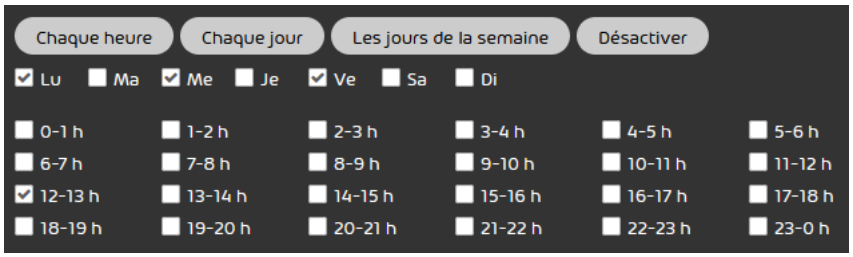


Illustration 45 : Sélectionner les heures

> **REMARQUE :**
>
> Aux moments de distribution sélectionnés, un rapport de quarantaine n'est envoyé que si de nouveaux courriels ont été mis en quarantaine depuis le dernier rapport de quarantaine.

Le filtre infomail et les rapports de quarantaine ont été configurés pour la boîte aux lettres.

Gestion des droits dans le Control Panel

Dans le Control Panel, un rôle est attribué à chaque utilisateur. Chaque rôle (voir Rôles à la page 49) dispose de certaines autorisations dans le Control Panel. Les droits sont répartis en différents domaines que les utilisateurs autorisés peuvent choisir dans la sélection de l'espace (voir Sélection de l' espace à la page 53).

Rôles

Dans le Control Panel, un rôle est attribué à chaque utilisateur. Chaque rôle dispose de certaines autorisations dans le Control Panel. En fonction de leurs autorisations, les utilisateurs ont accès à différentes zones du Control Panel (voir Sélection de l’ espace à la page 53).

Dans le Control Panel, les rôles suivants sont définis :

- **Utilisateur** : ce rôle est attribué automatiquement si aucun autre rôle n'a été attribué. Le rôle ne peut pas être attribué manuellement.
- **Administrateur** : ce rôle comporte des privilèges administratifs étendus.
- **Service Desk** : ce rôle est réservé au personnel d'assistance.
- **Reporting** : ce rôle n'a accès qu'aux statistiques.
- **Marketing** : ce rôle est réservé aux employés qui créent et modifient les signatures et les clauses de non-responsabilité. Le rôle peut être attribué en plus de l'un des autres rôles pour permettre à un employé d'accéder au module **Signature and Disclaimer**. Il n'est pas nécessaire d'attribuer le rôle en plus du rôle **Administrateur**, puisque les administrateurs ont déjà accès au module. Ce rôle n'est disponible qu'au niveau d'un client.
- **Security Awareness** : Ce rôle est réservé aux employés qui configurent et gèrent le Security Awareness Service pour un client. Le rôle peut être attribué en plus de l'un des autres rôles standards pour permettre à un employé d'accéder au module **Security Awareness Service**. Il n'est pas nécessaire d'attribuer le rôle en plus du rôle **Administrateur**, puisque les administrateurs ont déjà accès au module. Ce rôle n'est disponible qu'au niveau d'un client.

Le tableau indique à quels modules du Control Panel les rôles ont accès. **x** signifie que le rôle a accès au module.

Tableau 1 : Rôles et modules

MODULE	UTILISATEUR	ADMINISTRATEUR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Email Live Tracking	x	x	x			

MODULE	UTILISATEURS	ADMINISTRATEUR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Tableau de bord des services		x				
Rapports & conformité	x	x	x	x		
Web Filter		x				
Paramètres client		x				
Sauvegarde		x Les administrateurs côté clients ont accès à ce module uniquement si les administrateurs côté partenaires leur ont accordé l'accès.				
Blacklist & whitelist	x	x	x			

MODULE	UTILISATEUR	ADMINISTRATEUR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Security Awareness Service		x				x
Paramètres de sécurité		x			Le rôle n'a accès qu'au module **Signature and Disclaimer**.	
Personnalisation		x				
Paramètres utilisateur	x					

Les rôles qui ont accès au module **Email Live Tracking** disposent, à des degrés divers, d'actions sur les courriels. Le tableau suivant indique les actions sur les courriels (voir Actions sur les courriels à la page 89) que chacun de ces rôles peut effectuer.

REMARQUE :

Le tableau suivant contient également des actions qui ne sont disponibles qu'après la réservation de services supplémentaires et ne sont donc pas mentionnées dans le chapitre Actions sur les courriels à la page 89.

Tableau 2 : Rôle et actions sur les courriels

ACTION SUR LE COURRIEL	UTILISATEUR	ADMINISTRATEUR	SERVICE DESK
Libérer le courriel	x Les utilisateurs peuvent se faire remettre des courriels de la catégorie **Valide**. L'administrateur détermine si les utilisateurs peuvent se faire remettre des courriels d'autres catégories.	x	x
Restaurer le courriel	x	x	x
Signaler un spam	x	x	x
Signaler un infomail	x	x	x
Interdire l'expéditeur	x	x	x
Autoriser l'expéditeur et libérer le courriel	x	x	x
Interdire l'expéditeur pour tous les utilisateurs		x	
Autoriser l'expéditeur pour tous les utilisateurs		x	

ACTION SUR LE COURRIEL	UTILISATEUR	ADMINISTRATEUR	SERVICE DESK
Courriel à admin	X	X	X
Courriel au support	X	X	
Marquer comme confidentiel	X	X	X
Aperçu du courriel	X	Cette action n'est disponible pour les propres courriels de l'utilisateur que si l'utilisateur est sélectionné dans la plage de sélection.	Cette action n'est disponible pour les propres courriels de l'utilisateur que si l'utilisateur est sélectionné dans la plage de sélection.
Scan ATP		X	X
Rapport ATP		X	X
Info	X	X	X

Pour plus d'informations concernant la gestion des rôles, voir le chapitre « Administration des rôles et contacts » dans le manuel du Control Panel.

Sélection de l'espace

Par défaut, chaque utilisateur ne voit que ses propres paramètres et courriels dans le Control Panel. Cependant, les administrateurs et les autres utilisateurs qui ont un rôle avec des autorisations côté clients ou partenaires (voir Rôles à la page 49) peuvent changer l'espace d'application dans le Control Panel via la sélection de l'espace (voir Utilisation de la sélection de l'espace à la page 56) afin d'accéder aux paramètres d'un autre espace d'application. La sélection de l'espace est un menu déroulant situé en haut à droite du Control Panel.

REMARQUE :

Les utilisateurs simples ne peuvent pas changer d'espace d'application.

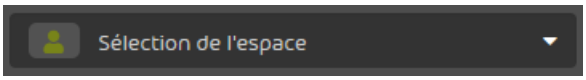


Illustration 46 : Sélection de l' espace

Si aucun domaine d'application n'est sélectionné dans la sélection de l'espace, le Control Panel affiche les paramètres et les courriels de l'utilisateur connecté et l'utilisateur peut gérer les paramètres de sa propre boîte aux lettres.

Les administrateurs et autres utilisateurs qui ont un rôle avec des autorisations côté clients ou partenaires peuvent, en fonction de leurs autorisations, accéder aux différents domaines d'application. Les domaines d'application sont organisés de manière hiérarchique et sont expliqués dans le tableau suivant.

Tableau 3 : Espaces de l’ application

ESPACE DE L’ APPLICATION	EXPLICATION
Partenaire	Les partenaires sont l'espace d'application le plus élevé dans le Control Panel. Des sous-partenaires ou des clients peuvent être subordonnés à un partenaire. **REMARQUE :** Aucun autre partenaire ne peut être créé dans les sous-partenaires, seulement des clients. Les administrateurs peuvent ajouter et supprimer des sous-partenaires et des clients dans cet espace d'application. Ce domaine d'application permet également de gérer des paramètres supérieurs qui sont transmis aux sous-partenaires et aux clients.

ESPACE DE L’APPLICATION	EXPLICATION
Client	Les clients sont des entreprises qui utilisent nos services. Un client est subordonné à un partenaire. Les clients sont gérés dans le Control Panel comme des domaines principaux. Les administrateurs peuvent consulter le trafic de courriels d’un client dans cet espace d’application. Les administrateurs peuvent également gérer les boîtes aux lettres, les groupes et les domaines alias du client ainsi que configurer nos services pour le client. Les expéditeurs interdits et autorisés du client peuvent également être gérés dans cet espace d’application. Les boîtes aux lettres sont subordonnées à un client et appartiennent à son domaine principal et à ses domaines alias.
utilisateur	Les utilisateurs sont l’espace d’application le plus bas du Control Panel. Les utilisateurs correspondent à des boîtes aux lettres. Un utilisateur est subordonné au client dont le domaine principal ou le domaine d’alias appartient à la boîte aux lettres. Dans cet espace d’application, les administrateurs peuvent voir le trafic de courriels de l’utilisateur. Les administrateurs peuvent également gérer les expéditeurs interdits et autorisés de l’utilisateur.

Utilisation de la sélection de l’espace

Si un autre rôle que celui d’utilisateur a été attribué à l’utilisateur, le Control Panel lui propose une possibilité simple pour basculer dans l’espace de l’application correspondant à votre rôle.

Dans la partie supérieure de la fenêtre se trouve la **Sélection de l’ espace** :

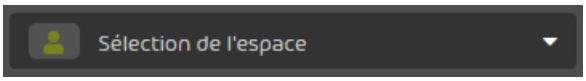


Illustration 47 : Sélection de l’ espace

La sélection de l'espace contient tous les espaces de l'application pour les rôles qui ont été attribués à l'utilisateur enregistré. Il existe deux possibilités pour sélectionner l'espace de l'application. La première possibilité consiste à sélectionner le partenaire, le client ou l'utilisateur directement dans le menu déroulant :

Illustration 48 : Sélection de l’ espace de l'application

La deuxième possibilité consiste à saisir le nom du partenaire, du client ou de l'utilisateur dans la barre de recherches.

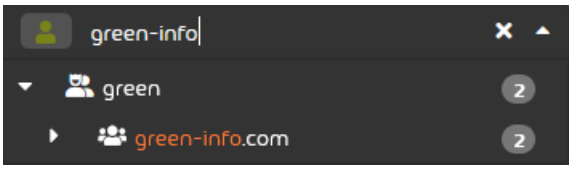


Illustration 49 : Recherche dans la sélection de l’ espace

Le nom du domaine recherché ne doit pas nécessairement être écrit en toutes lettres : il suffit de saisir une partie du nom pour limiter la liste de sélection aux éléments contenant cette suite de caractères.

Par défaut, la recherche est limitée aux partenaires et aux clients. Pour rechercher également des utilisateurs, la recherche d'utilisateurs doit être activée.

Illustration 50 : Activer la recherche d' utilisateurs

REMARQUE :

Dès que le caractère **@** a été saisi dans l'espace de recherche, la recherche d'utilisateurs est activée automatiquement.

Pour limiter la recherche à des partenaires et à des clients, la recherche d'utilisateurs doit être désactivée.

Illustration 51 : Désactiver la recherche d' utilisateurs

Email Live Tracking

Le module **Email Live Tracking** permet aux utilisateurs de surveiller leurs propres échanges de courriels et aux administrateurs de surveiller l'ensemble des échanges de courriels d'un client. Chaque utilisateur peut, indépendamment de ses autorisations, consulter les informations concernant ses propres courriels entrants et sortants et effectuer des actions sur les courriels. En plus des courriels de la boîte aux lettres principale apparaissent également les courriels des adresses alias.

Après leur connexion au Control Panel, les administrateurs voient directement aussi leurs propres courriels dans le module **Email Live Tracking**. Cependant, contrairement aux simples utilisateurs, les administrateurs peuvent changer l'affichage. Les administrateurs côté clientspeuvent voir le trafic de courriels de leur domaine principal et de leurs domaines alias.

REMARQUE :

Pour changer l'affichage, les administrateurs peuvent sélectionner un domaine ou un partenaire dans la sélection de l'espace en haut à droite du Control Panel. Si rien n'est sélectionné dans la sélection de l'espace, les administrateurs ne verront que leurs propres courriels dans le module **Email Live Tracking**.

Le module n'affiche que les courriels des domaines qui ont été vérifiés pour un client (voir Vérifications de domaines à la page 294).

Le module **Email Live Tracking** est structuré dans les trois domaines Filtre, Affichage des courriels et Statistiques par catégorie (voir Structure d' Email Live Trackings à la page 60).

Les utilisateurs peuvent adapter l'affichage des courriels dans le module (voir Modifier l' affichage des courriels à la page 62) ainsi que rechercher et filtrer les courriels affichés (voir Filtrer les courriels à la page 66). Le module **Email Live Tracking** contient des informations détaillées (voir Détails des courriels à la page 73) ainsi que des informations plus générales sur les courriels (voir Champs de courriel à la page 81). En outre, les courriels sont attribués à des catégories (voir Catégories de courriels à la page 84). Différentes actions peuvent être appliquées aux courriels (voir Actions sur les courriels à la page 89). En outre, les données de tous les courriels ou des

courriels sélectionnés peuvent être exportées sous forme de fichier CSV (voir Exporter les données de courriels sous un fichier CSV à la page 97).

Structure d’ Email Live Trackings

Ces domaines sont décrit ci-après.

Filtre

Vous pouvez filtrer vos courriels de différentes manières (voir Filtrer les courriels à la page 66).

Illustration 52 : Sélection des filtres

affichage des courriels

L'affichage des courriels est la fenêtre principale d'Email Live Tracking. Ici, tous les courriels sont affichés. Les filtres sélectionnés auparavant influent sur les courriels affichés.

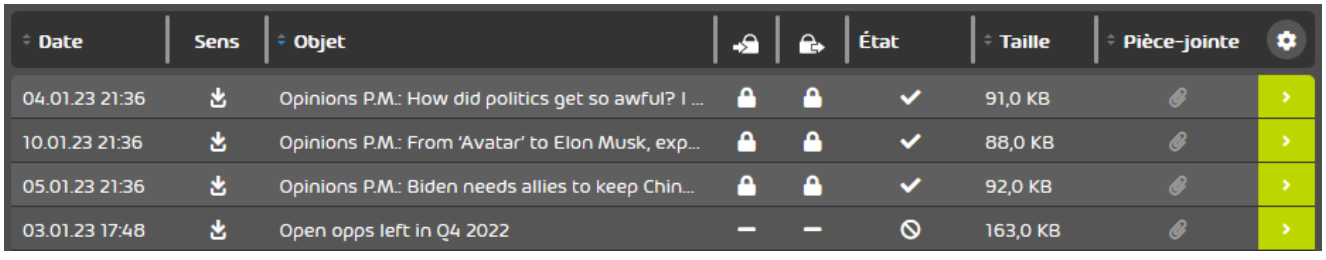


Illustration 53 : Affichage des courriels

Vous pouvez modifier l'affichage individuellement (voir Modifier l’ affichage des courriels à la page 62).

Tous les courriels correspondant aux filtres que vous avez réglés peuvent être exportés avec la fonction Exporter au format CSV. Dans ce cadre, vous pouvez sélectionner les champs à exporter (voir Exporter les données de courriels sous un fichier CSV à la page 97).

Il est possible d'effectuer des recherches dans de vastes listes de courriels à l'aide de la navigation sur les pages. La navigation sur les pages se trouve au centre de la partie basse de l'affichage. Le nombre d'éléments affichés par page peut être sélectionné dans le menu déroulant à droite. Pour accéder directement à une page spécifique, il est possible de saisir le numéro de la page dans le champ de saisie et d'ensuite confirmer en appuyant sur la touche Enter. Le nombre de pages disponibles apparaît à droite du champ de saisie. Les flèches simples à gauche et à droite du champ de saisie permettent de naviguer vers la page précédente ou suivante. Les doubles flèches permettent d'accéder à la première ou à la dernière page.

Illustration 54 : Navigation sur les pages

REMARQUE :

L'affichage est limité à 10 000 enregistrements, ce qui correspond à 200 pages avec les paramètres par défaut. Si plus de résultats ont été trouvés pour une requête, le nombre de pages disponibles est suivi d'un signe plus. Les fonctions de filtre (voir Filtrer les courriels à la page 66) peuvent limiter les courriels affichés afin d'obtenir des résultats plus précis.

Statistiques par catégorie

Les courriels dans l'Affichage des courriels sont évalués par catégories et apparaissent ensuite dans les statistiques. Vous pouvez afficher et cacher les statistiques avec la flèche à droite dans la partie basse de l'Affichage des courriels.

REMARQUE :

Les filtres appliqués sont pris en compte dans les statistiques.

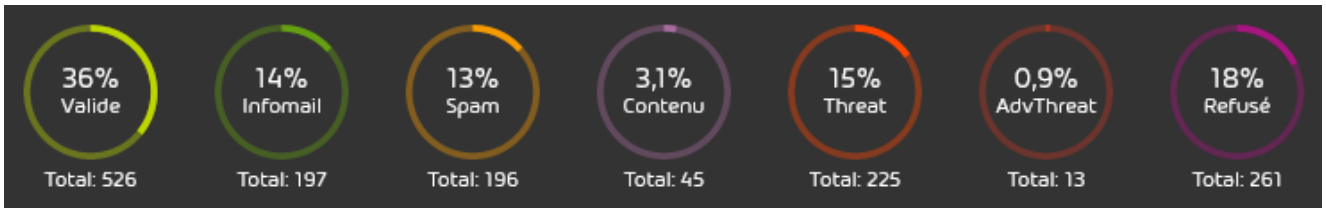


Illustration 55 : Statistiques par catégorie

Modifier l'affichage des courriels

Les utilisateurs disposent des possibilités suivantes pour personnaliser l'affichage des courriels :

- Sélectionner les champs qui doivent apparaître (voir Personnaliser les colonnes affichées à la page 62).
- Modifier la taille des champs (voir Modifier la taille des champs à la page 64).
- Modifier les positions des champs (voir Modifier l'ordre des champs de courriel à la page 65).

Personnaliser les colonnes affichées

Le module **Email Live Tracking** (voir Email Live Tracking à la page 59) contient un aperçu de vos courriels entrants et sortants.

REMARQUE :

Les administrateurs côté clients peuvent consulter les courriels de leur domaine principal et de leurs domaines alias au lieu de leurs propres courriels s'ils sélectionnent le domaine dans la sélection de l'espace en haut à droite dans le Control Panel.

Les courriels sont affichées dans un tableau. Le tableau contient des informations sur les courriels. Vous pouvez choisir les informations qui seront affichées dans le module **Email Live Tracking**. Pour plus d'informations concernant les colonnes disponibles, voir Champs de courriel à la page 81.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Naviguez vers le module **Email Live Tracking**

3. Cliquez sur le symbole de tableau en haut à droite dans le tableau.

Illustration 56 : Ouvrir les champs de courriel

Une liste des champs de courriel disponibles apparaît.

4. Sélectionnez les champs de votre choix.

REMARQUE : Le fond des champs sélectionnés est bleu.

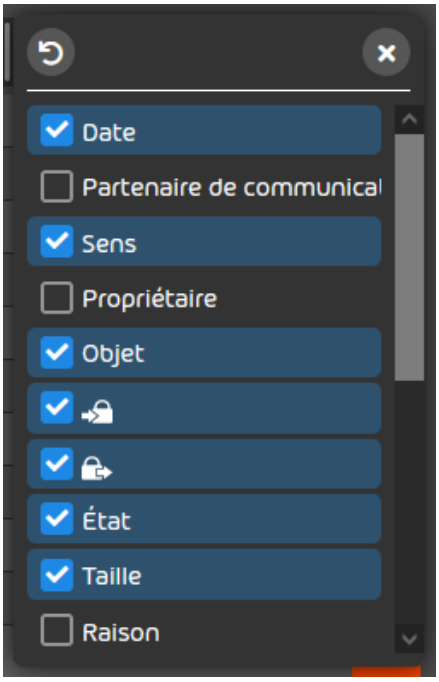


Illustration 57 : Sélectionner les champs de courriel

Les champs de courriel affichés ont été adaptées.

Vous pouvez ensuite modifier la taille des champs affichés (voir Modifier la taille des champs à la page 64) et modifier l'ordre des champs (voir Modifier l' ordre des champs de courriel à la page 65).

Modifier la taille des champs

Vous avez adapté les informations des courriels affichées (voir Personnaliser les colonnes affichées à la page 62).

Vous pouvez modifier la taille des champs dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Naviguez vers le module **Email Live Tracking**
3. Placez le curseur de la souris entre deux champs.

Illustration 58 : Modifier la taille

Une ligne bleue apparaît entre les champs.

4. Tirez le champ vers la gauche ou la droite à la taille désirée.

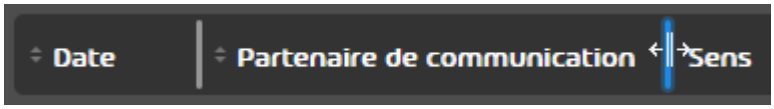


Illustration 59 : Modifier la taille

La taille des champs a été modifiée.

Vous pouvez ensuite modifie l'ordre des champs (voir Modifier l' ordre des champs de courriel à la page 65).

Modifier l’ ordre des champs de courriel

Vous avez adapté les informations des courriels affichées (voir Personnaliser les colonnes affichées à la page 62).

Vous pouvez modifier l'ordre des champs de courriel dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Naviguez vers le module **Email Live Tracking**
3. Cliquez sur un champ et maintenez le bouton de la souris enfoncé.

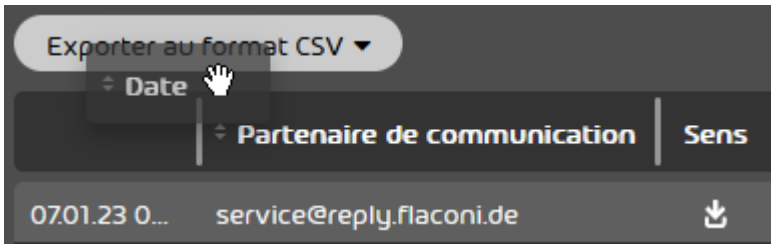


Illustration 60 : Modifier ordre 1

4. Tirez le champ jusqu'à la position désirée et relâchez le bouton de la souris.

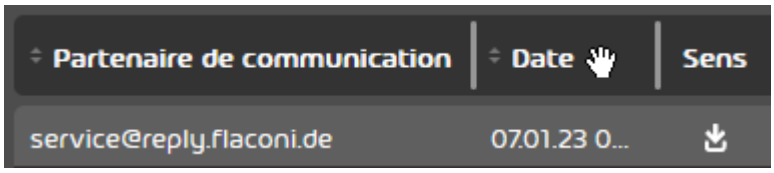


Illustration 61 : Modifier ordre 2

L'ordre des champs de courriel a été modifié.

Vous pouvez ensuite modifier la taille des champs (voir Modifier la taille des champs à la page 64).

Filtrer les courriels

La recherche de courriels permet de filtrer les courriels affichés dans la vue d'ensemble et de rechercher des courriels précis. Les possibilités suivantes sont disponibles :

- Filtrer les courriels par catégories (voir Filtrer les courriels par catégories à la page 66).
- Utiliser d'autres filtre de courriels (voir Filtre de champ à la page 70).
- Rechercher des courriels via la barre de recherche et limiter la recherche à des champs spécifiques (voir Barre de recherches à la page 67).
- Réinitialiser ou répéter la recherche (voir Réinitialiser ou répéter la recherche à la page 72).
- Utiliser la fonction de recherche avancée (voir Fonction de recherche élargie à la page 69)

Filtrer les courriels par catégories

Vous pouvez filtrer les courriels par catégories dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez afficher les courriels.
3. Naviguez vers le module **Email Live Tracking**.

4. Activez ou désactivez les catégories désirés dans le menu de filtre.

> **REMARQUE :**
>
> Pour afficher seulement les courriels d'une catégorie précise, double-cliquez sur la catégorie désirée. Toutes les autres catégories sont alors désactivées.

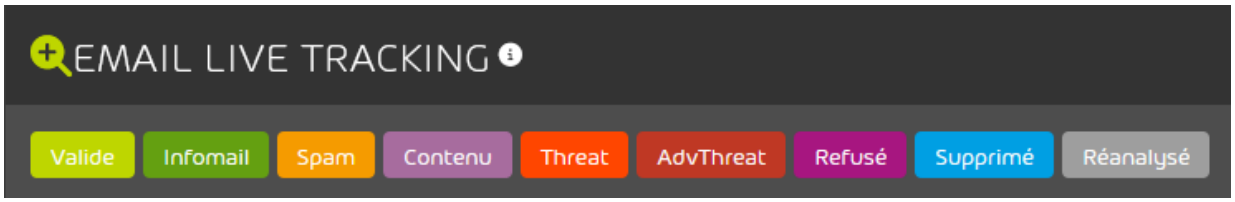


Illustration 62 : Désactiver/activer les catégories de courriels

Seuls les courriels des catégories actives sont affichés dans le tableau.

Les courriels du module **Email Live Tracking** ont été filtrés par catégories.

Barre de recherches

Une saisie dans la barre de recherche du module **Email Live Tracking** (voir Email Live Tracking à la page 59) permet aux utilisateurs de chercher des courriels (voir Parcourir les courriels à la page 67). Une option permet de limiter la recherche à des champs spécifiques (voir Limiter la recherche à certains champs à la page 68). En outre, la barre de recherche contient une fonction de recherche avancée pour compléter les demandes de recherche (voir Fonction de recherche élargie à la page 69).

Parcourir les courriels

Vous pouvez rechercher les courriels dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59).

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Facultatif : Si vous souhaitez rechercher les courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.

3. Naviguez vers le module **Email Live Tracking**
4. Saisissez une suite de caractères dans le champ de recherche.

> **IMPORTANT :**
>
> Vous devez saisir au moins trois caractères afin de pouvoir utiliser la recherche.

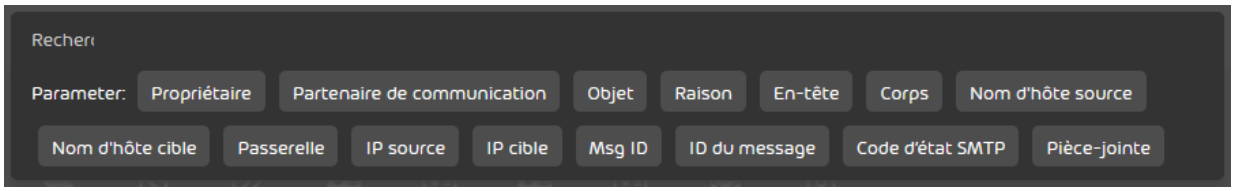


Illustration 63 : Barre de recherches

Les résultats sont modifiés en temps réel.

Les courriels du module **Email Live Tracking** ont été consultés.

Limiter la recherche à certains champs

Dans le module **Email Live Tracking** (voir Parcourir les courriels à la page 67), vous pouvez limiter la recherche de courriels à certains champs ; seuls ces champs sont recherchés pour la série de caractères saisie.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Facultatif : Si vous souhaitez rechercher les courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers le module **Email Live Tracking**
4. Sélectionnez un champ parmi les propositions de la recherche.

5. Saisissez une série de caractères à rechercher dans le champ sélectionné.

Illustration 64 : Limiter la recherche à certains champs

La recherche de courriels a été limitée à certains champs.

Fonction de recherche élargie

Avec la recherche en texte intégral dans le module, tous les champs des courriels sont parcourus. De plus, il est possible de parcourir les différents champs des courriels de manière combinée.

La recherche dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) complète les demandes de recherche. Afin, les utilisateurs peuvent uniquement rechercher avec des débuts de mots. La recherche au sein des mots n'est pas prévue.

Dans les champs des courriels, différents caractères de séparation sont utilisés pour séparer les mots les uns des autres.

Dans le tableau suivant, des exemples de demandes de recherche valides et non valides sont donnés. Pour cela, les caractères de séparation des champs des courriels indiqués sont décrits.

REMARQUE :

Les pièces-jointes ne sont parcourues que si la recherche a été limitée au champ **Pièce-jointe** (voir Limiter la recherche à certains champs à la page 68).

Tableau 4 : Exemples de demandes de recherche complexes

TYPE	CARACTÈRE DE SÉPARATION	EXEMPLE	DEMANDE DE RECHERCHE VALIDE	DEMANDE DE RECHERCHE NON VALIDE
Adresse courriel	« @ » et « . » dernier	info@test.de	info; test; de	o@test; nfo@
Hostname	« - » et « . »	gateway07-rz01.test.de	gate; rz01; test; de	eway; 07; 01;
Pièces-jointes	","	text.txt; image.jpg	text.txt; image.jpg	text; txt; xt; mage; image; jpg; pg
Texte courant	Caractère spécial	Nous assurons la sécurité informatique de nos clients – avec les services de Cloud Security, dans le monde entier, 24 h sur 24.	nous; assurons; sécuri; entier	curité; ervices; ans
Raison	« : »	linktag: lt_exprx_15_10_442: auto	linktag; lt_exprx; auto	tag; exprx; 10_442

Filtre de champ

Dans le module **Email Live Tracking**, les filtres **Date**, **Sens**, **Cryptage**, **État de distribution** et **Taille** peuvent être appliqués. Ceux-ci sont expliqués dans le tableau ci-dessous.

Tableau 5 : Filtre

PROPRIÉTÉ	DESCRIPTION
Date	Sélectionnez une période dans le menu déroulant ou limitez l'affichage à une plage temporelle. Le réglage par défaut est **Aujourd'hui**. Si une période (**Le mois dernier**, **Cette année** etc.) est sélectionnée, le fuseau horaire UTC est utilisé par défaut, quels que soient les paramètres de l'utilisateur. Si un fuseau horaire autre que l'UTC est défini pour l'utilisateur, les courriels du dernier jour civil avant la période sélectionnée peuvent donc également être affichés dans l'affichage des courriels. **REMARQUE :** L'intervalle de temps ne doit pas être supérieur à 365 jours. Le menu déroulant ne permet pas de sélectionner des intervalles de temps plus longs. La saisie manuelle d'un intervalle de temps plus long entraîne un message d'erreur.
Sens	Sélectionnez si les courriels entrants ou les courriels sortants doivent être affichés. Dans le paramètre par défaut, les deux sens sont affichés.
Cryptage	Limitez l'affichage aux courriels ayant un type de cryptage précis. Vous pouvez sélectionner plusieurs types de cryptage.

PROPRIÉTÉ	DESCRIPTION
État de distribution	Déterminez le statut des courriels qui doivent être affichés. Les statuts suivants peuvent être sélectionnés : **Libéré**, **Retardé**, **Refusé** et **Aucun état**.
Taille	Limitez les courriels à une taille précise. Sélectionnez la taille dans le menu déroulant.

Réinitialiser ou répéter la recherche

Vous avez effectué une recherche dans le module **Email Live Tracking** (voir Parcourir les courriels à la page 67 ou Limiter la recherche à certains champs à la page 68) et/ou appliqué certains filtres de champ (voir Filtre de champ à la page 70) et vous êtes toujours dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59).

Après avoir effectué une recherche des courriels du module **Email Live Tracking**, vous pouvez soit réinitialiser vos paramètres de recherche (voir Parcourir les courriels à la page 67, Limiter la recherche à certains champs à la page 68 et Filtre de champ à la page 70), soit effectuer une nouvelle recherche avec vos paramètres de recherche actuels pour mettre à jour les résultats de la recherche.

Réinitialisez vos paramètres de recherche ou effectuez une nouvelle recherche avec vos paramètres de recherche actuels. Pour cela, cliquez sur l'un des boutons suivants :

- **Réinitialiser** : les paramètres de recherche sont réinitialisés.
- **Mettre à jour** : une nouvelle recherche est effectuée avec les paramètres de recherche actuels.

Illustration 65 : Réinitialiser les paramètres de recherche ou relancer la recherche

Les paramètres de recherche ont été réinitialisés ou la recherche a été relancée avec les paramètres de recherche actuels.

Détails des courriels

L'affichage des courriels dans le **Email Live Tracking** (voir Email Live Tracking à la page 59) affiche les détails des différents courriels.

Il est également possible d'effectuer des actions pour le courriel sélectionné via les détails du courriel (voir Effectuer une action pour un seul courriel à la page 73). Les actions suivantes peuvent être exécutées :

- Signaler le courriel comme courriel indésirable (voir **Signaler un spam**)
- Signaler le courriel comme infomail (voir **Signaler un infomail**)
- Envoyer le courriel (voir **Libérer le courriel**)
- Effectuer un scan ATP (voir Démarrer le rapport ATP à la page 75)

En fonction des produits activés et des actions validées par l'administrateur, d'autres actions peuvent être disponibles (voir Actions sur les courriels à la page 89).

Les métadonnées, les en-têtes et le dialogue SMTP du courriel peuvent être visualisés dans les détails du courriel (voir Informations élargies des courriels à la page 79).

Effectuer une action pour un seul courriel

Si vous souhaitez effectuer une action pour un seul courriel, procédez de la manière suivante.

> **REMARQUE :**
>
> Vous pouvez également effectuer une action pour plusieurs courriels (voir Sélectionner un action pour plusieurs courriels à la page 87).

1. Connectez-vous au Control Panel.
2. Facultatif : Si vous souhaitez accéder aux courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers le module **Email Live Tracking**.

4. Cliquez sur la flèche à la fin de la ligne désirée du courriel.

> **REMARQUE :**
>
> La couleur indique la catégorie du courriel.

Un menu s'ouvre.

5. Cliquez sur l'action que vous souhaitez exécuter.

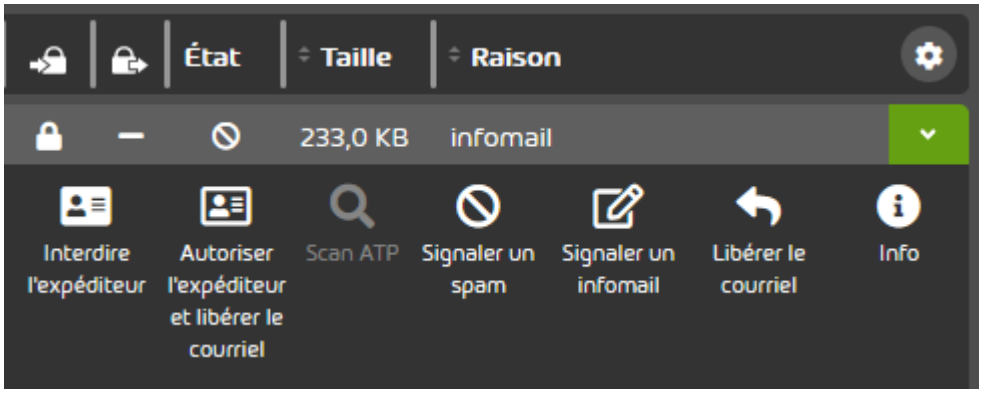


Illustration 66 : Actions sur les courriels

> **REMARQUE :**
>
> D'autres actions sont disponibles dans la sélection des courriels (voir Sélectionner un action pour plusieurs courriels à la page 87).

> **REMARQUE :**
>
> Vous trouverez une explication des actions des courriels sous Actions sur les courriels à la page 89.

Une action a été effectuée pour un seul courriel.

Démarrer le rapport ATP

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365).

Le rapport ATP (voir le chapitre « Rapport ATP » dans le manuel du Control Panel) vous permet d'analyser manuellement les courriels avec des pièces jointes exécutables dans le module **Email Live Tracking** (voir le chapitre « Email Live Tracking » dans le manuel du Control Panel) pour détecter les contenus malveillants.

REMARQUE :

Le rapport ATP n'est possible que pour les courriels comportant des pièces jointes exécutables (par exemple, des fichiers .exe).

ATTENTION :

Si vous n'avez pas souscrit à l'Advanced Threat Protection (voir le chapitre « Structure et fonction d'ATP » dans le manuel du Control Panel), vous pouvez bénéficier gratuitement de deux rapports ATP par mois. Vous ne pouvez effectuer d'autres rapports ATP que si vous avez souscrit à l'ATP payant.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Si vous souhaitez accéder aux courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers le module **Email Live Tracking**.

4. Cliquez sur la flèche à droite du courriel souhaité.

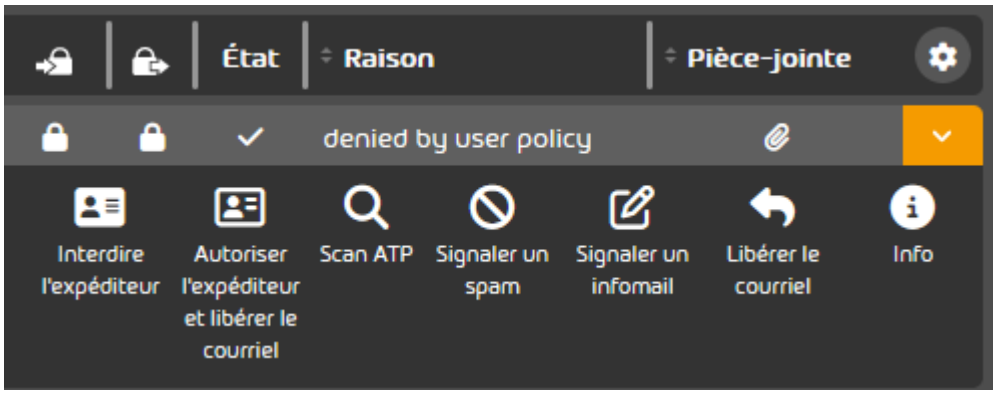


Illustration 67 : Rapport ATP dans Email Live Tracking

L'écran des fonctions étendues s'ouvre.

5. Cliquez sur **Scan ATP** pour lancer le rapport.

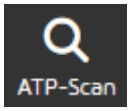


Illustration 68 : Démarrer le rapport ATP

Le rapport ATP a été lancé pour le courriel.

Une fois le rapport ATP terminé, vous pouvez consulter le rapport ATP dans la vue des fonctionnalités avancées du courriel sous la rubrique **Scan ATP** (voir Rapport ATP à la page 77).

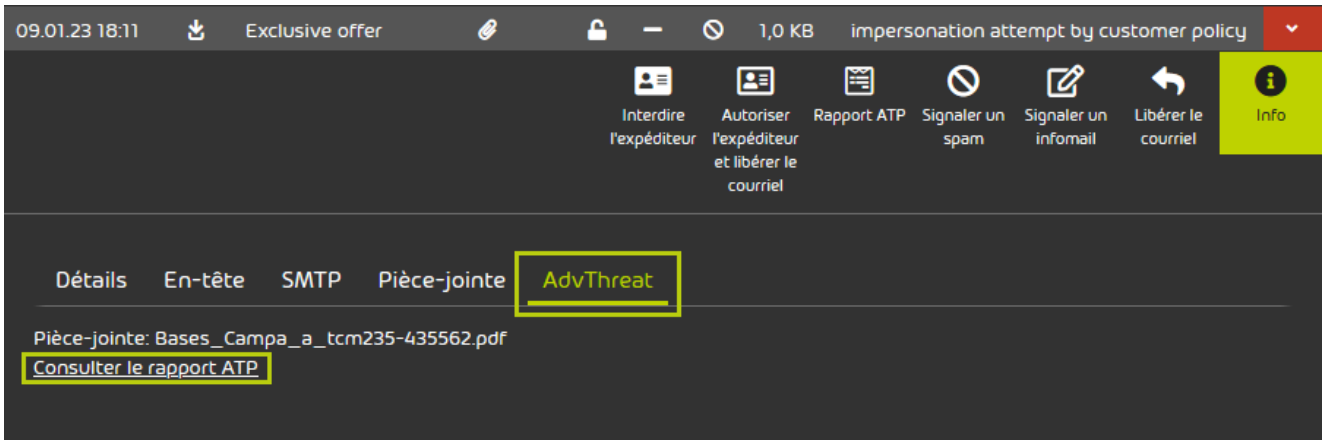


Illustration 69 : Ouvrir le rapport ATP

Rapport ATP

Le rapport ATP est un rapport détaillé qui est généré dès qu'un courriel a été vérifié avec le rapport ATP (voir le chapitre « Rapport ATP » dans le manuel du Control Panel et Démarrer le rapport ATP à la page 75). Le rapport ATP fournit des informations sur le courriel contrôlé. Les rapports ATP sont disponibles dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) pour les courriels vérifiés. Le rapport ATP d'un courriel peut être consulté dans le menu de courriel sous le point de menu **Rapport ATP** ou **Info** dans l'onglet **AdvThreat**.

Le rapport ATP est divisé en quatre fenêtres principales :

Summary

Vous trouverez ici un aperçu du fichier analysé. En outre, un **Score** de 0 à 10 est attribué au fichier. 0 signifie aucun danger et 10 est le niveau de danger le plus élevé.

Dans la section **Signatures**, le fichier est classé dans l'une des catégories suivantes en fonction de son comportement :

- information (vert)
- attention (jaune)
- avertissement (rouge)

Si vous cliquez sur une signature, les informations élargies au processus étendu s'affichent.

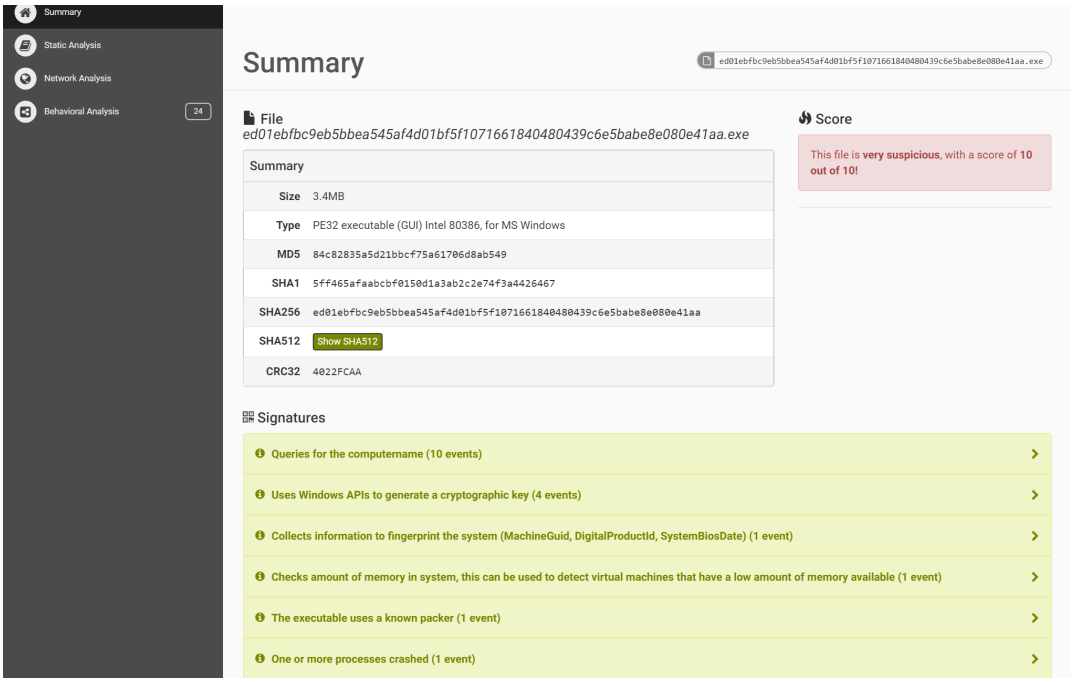


Illustration 70 : Aperçu rapport ATP

Static Analysis

L'analyse statique est à nouveau divisée en trois sous-catégories :

- Static Analysis – Analyse statique du fichier. Selon le format du fichier.
- Strings – Sortie des chaînes de caractères du fichier.
- Antivirus – Analyse du fichier par différents programmes antivirus.

Network Analysis

Dans l'analyse du réseau, l'ensemble du trafic réseau est analysé et répertorié selon les protocoles (par exemple HTTP, TCP, UDP).

Behavioral Analysis

L'analyse du comportement analyse le comportement du fichier au moment de l'exécution.

Tous les appels et processus de l'API système qui ont été enregistrés pendant l'analyse dynamique sandbox sont affichés.

Les résultats sont divisés en deux sections :

- Process Tree – Ici, les processus sont affichés dans l'ordre hiérarchique.
- Process Contents – Si vous sélectionnez un processus dans l'arborescence des processus, les requêtes API exécutées sont affichées ici par ordre chronologique.

Informations élargies des courriels

Dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59), dans les détails des courriels sous **Info**, se trouvent des informations sur le courriel sélectionné. Les informations détaillées sur un courriel sont réparties dans les sections **Détails**, **En-tête**, **SMTP** et, le cas échéant,**Pièce-jointe**.

Détails

Cette catégorie contient les informations suivantes sur le courriel sélectionné :

- **Propriétaire** : Utilisateur du Control Panel qui a reçu ou envoyé le courriel
- **Partenaire de communication** : Partenaire de communication du propriétaire du courriel (peut être destinataire et expéditeur)
- **Cryptage des courriels entrants** : Méthode de cryptage des courriels entrants du point de vue de notre serveur. Ces courriels proviennent des utilisateurs du Control Panel ou de leurs partenaires de communication et arrivent sur nos serveurs.
- **Cryptage des courriels sortants** : Méthode de cryptage des courriels sortants du point de vue de notre serveur. Ces courriels sont envoyés par nos serveurs aux utilisateurs du Control Panel ou à leurs partenaires de communication.
- **Catégorie** : Catégorie attribuée au courriel dans le Control Panel (voir Catégories de courriels à la page 84)
- **Objet** : Objet du courriel
- **Raison** : Motif de catégorisation du courriel (voir Raisons de catégorisation à la page 627)
- **Nom d'hôte source** : Nom du serveur de l'expéditeur

- **ID du message** : Identification du courriel attribuée par le serveur d'origine de l'expéditeur
- **Code d' état SMTP** : Informations de la dernière réponse de notre serveur dans le dialogue SMTP. Ces informations sont affichées dans les courriels avec le statut de distribution **Libéré** ou **Retardé** (voir Filtre de champ à la page 70). Cela comprend les informations suivantes :
  - Horodatage de la transaction
  - Protocole utilisé (SMTP, TLS ou EMIG)
  - Nom d'hôte et adresse IPv4 du serveur de réception
  - Code SMTP et, le cas échéant, message SMTP
  - **END-SEND** : Cette valeur indique que le client SMTP a émis la commande SMTP **QUIT**. La valeur indique que la communication a été terminée correctement.
  - **CIPHER** : Ce champ n'apparaît que si TLS est utilisé et fait référence à la puissance des algorithmes de cryptage utilisés. Les valeurs possibles sont **NONE** (si la communication a eu lieu sur un canal non crypté), **WEAK** (si la communication a eu lieu avec une version de TLS antérieure à 1.2 ou avec un algorithme de cryptage que nous considérons comme faible) et **STRONG** (autres).
  - **IDENTITY**: Ce champ ne s'affiche que si TLS est utilisé et fait référence à la méthode d'authentification utilisée. La valeur **NONE** indique que la communication a eu lieu sur un canal non crypté. La valeur **EMIG_VERIFIED** indique que l'authentification a eu lieu via EmiG. La valeur **CA_VERIFIED** indique que le certificat TLS du partenaire de communication a été validé. La valeur **SELF_ISSUED** indique que le certificat TLS du partenaire de communication n'a pas été validé, soit parce qu'il est auto-signé, soit parce que la validation n'est que partielle.
- **Domaine du propriétaire** : Domaine de l'utilisateur qui a reçu ou envoyé le courriel.

> **REMARQUE :**
>
> Pour les anciens courriels qui ont été reçus ou envoyés avant l'implémentation de la procédure de vérification des domaines (voir « Vérifications de domaines » dans le manuel du Control Panel), ce champ est vide.

En-tête

La section Header du courriel sélectionné est affichée ici. L'en-tête des courriels rejetés ne peut pas être affichée.

SMTP

Cette section affiche le résultat de la transmission du courriel. Pour de plus amples informations, voir la déclaration sous **Détails** > **Code d' état SMTP**. S'il y a eu plusieurs tentatives de distribution, plusieurs messages seront affichés ici.

Pièce-jointe

Un tableau contenant les pièces jointes du courriel est affiché ici. Pour chaque pièce jointe, le nom du fichier apparaît dans la colonne **Pièce-jointe** et la valeur de hachage apparaît dans la colonne **Hash de la pièce-jointe**.

Champs de courriel

Dans le tableau suivant sont décrites les colonnes qui peuvent être affichées dans le tableau des courriels du module **Email Live Tracking** (voir Email Live Tracking à la page 59). Les noms et les significations des colonnes correspondent en grande partie aux champs des informations sur les courriels (voir Informations élargies des courriels à la page 79).

Tableau 6 : Champs de courriel

CHAMP	DESCRIPTION
Passerelle	Passerelle utilisée
Objet	Objet du courriel
Raison	Motif de catégorisation du courriel (voir Raisons de catégorisation à la page 627)

CHAMP	DESCRIPTION
Partenaire de communication	Partenaire de communication du propriétaire du courriel (peut être destinataire et expéditeur) **REMARQUE :** Le champ contient l'entête From pour les courriels entrants et l'entête To du courriel pour les courriels sortants. Pour les courriels entrants de la catégories **Refusé**, le champ contient l'Envelope From du courriel. L'Envelope From peut contenir une chaîne de caractères différente d'une adresse courriel.
Nom d'hôte source	Nom du serveur de l'expéditeur
Propriétaire	Utilisateur du Control Panel qui a reçu ou envoyé le courriel **REMARQUE :** Le champ contient l'entête To pour les courriels entrants et l'entête From du courriel pour les courriels sortants. Pour les courriels entrants de la catégories **Refusé**, ce champ contient l'Envelope To du courriel.
Nom d'hôte cible	Nom du serveur du destinataire

CHAMP	DESCRIPTION
IP cible	Adresse IP du destinataire (uniquement pour les courriels envoyés)
ID du message	Identification du courriel attribuée par le serveur d'origine de l'expéditeur
IP source	Adresse IP de l'expéditeur
Msg ID	Identification du courriel qui a été attribuée par nos serveurs
Date	Date et heure du courriel
Sens	Le sens du message du point de vue du propriétaire.  signifie « entrant » et  signifie « sortant ».
	Méthode de cryptage des courriels entrants du point de vue de notre serveur. Ces courriels proviennent des utilisateurs du Control Panel ou de leurs partenaires de communication et arrivent sur nos serveurs. Un symbole de verrou indique que le courriel entrant est crypté. Pour connaître la méthode de cryptage du courriel, passez avec la souris sur le symbole du verrou ou ouvrez les Détails du courriel.

CHAMP	DESCRIPTION
	Méthode de cryptage des courriels sortants du point de vue de notre serveur. Ces courriels sont envoyés par nos serveurs aux utilisateurs du Control Panel ou à leurs partenaires de communication. Le statut de cryptage et la méthode de cryptage s'affichent de la même manière qu'avec 
État	Statut de livraison du courriel (voir Filtre de champ à la page 70)
Taille	Taille du courriel, pièce-jointe incluse
Pièce-jointe	Un symbole indique si le courriel contient des pièces jointes.

Catégories de courriels

Les courriels des utilisateurs sont répartis dans les catégories suivantes dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) :

Tableau 7 : Catégories de courriels

CATÉGORIE	DESCRIPTION
Valide	Ces courriels sont supposés être souhaités par le destinataire et ne pas constituer une menace pour lui.

CATÉGORIE	DESCRIPTION
Infomail	Ces courriels sont à caractère publicitaire. Les infomails incluent également les newsletters envoyées par courriel. Vous pouvez classifier les courriels de cette catégorie comme **Spam** ou **Valide**. Dans les cas suivants, un courriel n'est pas classifié directement comme **Valide**, mais comme **Infomail** : • Le courriel provient d'un expéditeur de newsletter connu. • Les newsletters sont envoyées régulièrement par la plage d'IP de l'expéditeur. • Le courriel présente un mot-clé ou une chaîne de caractères indiquant qu'il s'agit d'une newsletter. • Le courriel présente plusieurs caractéristiques qui, combinées, indiquent qu'il s'agit d'une newsletter.
Spam	Ces courriels ne sont pas souhaités et présentent souvent un caractère publicitaire ou malveillant. Les courriels sont envoyés simultanément à un grand nombre de destinataires.
Contenu	Ces courriels ont une pièce jointe non conforme. La nature non conforme des pièces jointes est définie par les administrateurs dans le module **Content Control**.

CATÉGORIE	DESCRIPTION
Threat	Ces courriels présentent des contenus dangereux, comme des pièces jointes ou des liens malveillants, ou sont envoyés pour commettre des infractions, telles que le phishing.
AdvThreat	Advanced Threat Protection a identifié ces courriels comme une menace. Les courriels sont utilisés à des fins illégales et font appel à des moyens techniques sophistiqués qui ne peuvent être contrés qu'à l'aide de procédures dynamiques avancées.
Refusé	Ces courriels sont refusés par notre serveur de messagerie et ne sont pas analysés davantage dans le cadre du dialogue SMTP, en raison de caractéristiques externes, comme l'identité de l'expéditeur.
Réanalysé	Dans le cas peu probable où les courriels seraient par exemple mis en quarantaine dans une mauvaise catégorie en raison d'un réglage trop stricte du filtre, nos administrateurs peuvent lancer une nouvelle analyse des courriels concernés une fois la cause première éliminée. Si ces courriels ne sont plus considérés comme une menace, ils sont envoyés au destinataire et classés comme **Réanalysé**.

Sélectionner un action pour plusieurs courriels

Si vous souhaitez effectuer une action simultanément pour plusieurs courriels dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59), procédez de la manière suivante.

REMARQUE :

Vous pouvez également effectuer cette action uniquement pour un courriel distinct (voir Effectuer une action pour un seul courriel à la page 73).

1. Connectez-vous au Control Panel.
2. Si vous souhaitez accéder aux courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers le module **Email Live Tracking**.
4. Cliquez sous le bouton sous les filtres pour ouvrir une barre avec les actions.

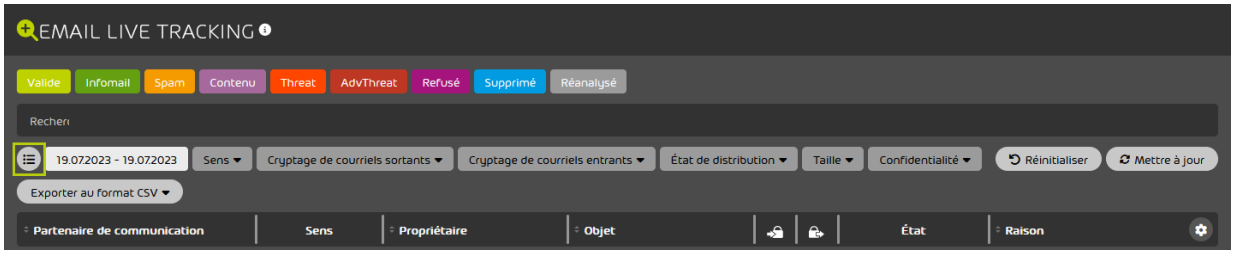


Illustration 71 : Ouvrir des actions

5. Cliquez sur les courriels désirés pour les sélectionner.

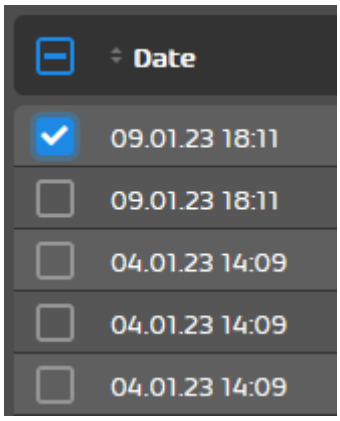


Illustration 72 : Sélectionner un courriel

REMARQUE :

Vous pouvez également sélectionner simultanément tous les courriels affichés.

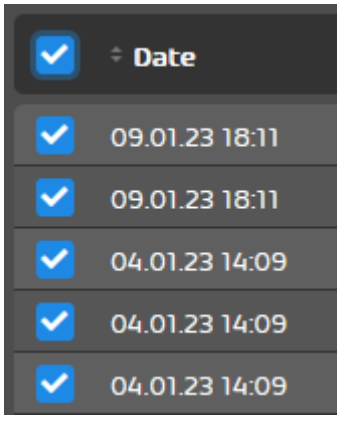


Illustration 73 : Sélectionner tous les courriels affichés

6. Cliquez sur une action pour l'exécuter pour les courriels sélectionnés.

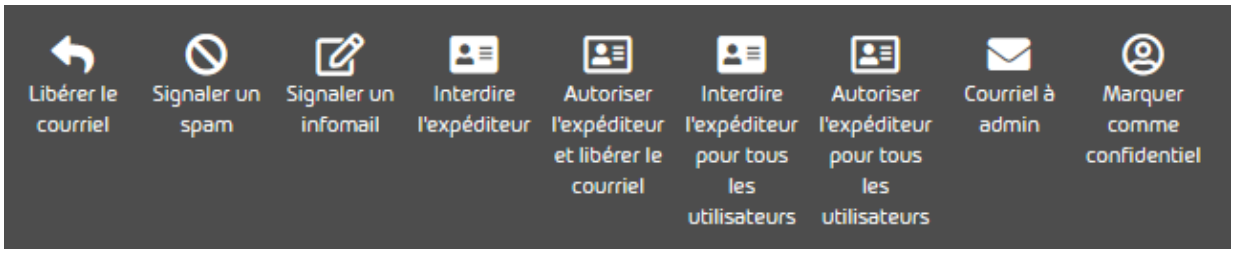


Illustration 74 : Sélectionner une action

L'action est appliquée aux courriels sélectionnés.

Une action a été effectuée simultanément pour plusieurs courriels.

Actions sur les courriels

Pour les courriels dans le module **Email Live Tracking**, il est possible d'effectuer différentes actions, comme par ex. les interdire. Le tableau suivant décrit les actions qui peuvent être effectuées pour les courriels dans le module **Email Live Tracking**.

REMARQUE :

La disponibilité des actions sur les courriels dépend des actions qui ont été déverrouillées par l'administrateur et des produits qui sont activés.

Tableau 8 : Actions sur les courriels

ACTION	DESCRIPTION
Libérer le courriel	Les courriels sélectionnés sont envoyés au destinataire. Cette action est disponible pour les courriels des catégories **Valide**, **Infomail**, **Spam**, **Contenu**, **Threat** et **AdvThreat**. Pour les courriels des catégories **Spam**, **Contenu**, **Threat** et **AdvThreat**, un processus de réévaluation de la catégorisation est déclenché en plus de l'envoi. Pour les utilisateurs, l'action n'est disponible pour les courriels des catégories **Infomail**, **Spam**, **Contenu** et **Threat** que si l'administrateur a activé la distribution (voir Autoriser ou interdire les actions d' utilisateur à la page 469). Seuls les administrateurs et les utilisateurs avec le rôle **Service Desk** peuvent distribuer des courriels de la catégorie **AdvThreat**. La ligne supplémentaire **x-hornetsecurity-delivered:** avec des informations sur le rôle de l'utilisateur qui a déclenché cette action est ajoutée à l'entête des courriels distribués. Le personnel d'assistance, les administrateurs côté partenaires, les administrateurs côté clients et les simples utilisateurs sont chacun identifiés par les mots **support**, **reseller**, **admin** et **user**.

ACTION	DESCRIPTION
Aperçu du courriel	Une nouvelle fenêtre propose un lien crypté permettant d'accéder à un service web où le contenu du courriel sélectionné s'affiche de manière sécurisée. Les images, liens et autres contenus actifs provenant du courriel sont désactivés ou remplacés par des caractères de remplacement sécurisés. Si nécessaire et dans la mesure du possible, la mise en page et le codage du courriel sont légèrement modifiés pour afficher le contenu du courriel. **REMARQUE :** Cette action est visible uniquement si aucun domaine d'application n'est sélectionné dans la sélection de l'espace et si les courriels de la boîte aux lettres de l'utilisateur connecté sont affichés dans l'Email Live Tracking (voir Sélection de l'espace à la page 53). **REMARQUE :** Les utilisateurs du Control Panel peuvent appliquer cette action aux courriels dont ils sont propriétaires. Les remplaçants peuvent en également afficher une prévisualisation des courriels de la boîte aux lettres pour laquelle ils sont enregistrés en tant que remplaçant (voirSaisir une délégation à la page 245). **REMARQUE :** Ces actions ne sont disponibles que pour certaines courriels (voir Effectuer

ACTION	DESCRIPTION
Signaler un spam	Les courriels sélectionnés sont signalés au système de support et de gestion de la qualité et sont à nouveau catégorisés. Il s'agit de la méthode privilégiée de gestion des courriels mal catégorisés. **REMARQUE :** L'action sur les courriels **Signaler un spam** permet de signaler tous les courriels qui ont été mal catégorisés (faux-négatifs).
Signaler un infomail	Les courriels sélectionnés sont classés comme infomail. Les paramètres de gestion des infomails peuvent être modifiés individuellement.
Interdire l'expéditeur	Les expéditeurs des courriels sélectionnés sont interdits pour l'utilisateur. Les autres courriels des expéditeurs seront automatiquement classés dans le courriel indésirable.
Autoriser l'expéditeur et libérer le courriel	Les expéditeurs des courriels sélectionnés sont autorisés pour l'utilisateur et les courriels sont distribués. Tous les autres courriels des expéditeurs seront automatiquement distribués.
Interdire l'expéditeur pour tous les utilisateurs	Les expéditeurs des courriels sélectionnés sont interdits pour tous les utilisateurs du domaine et les courriels entrants sont classés dans le courriel indésirable.

ACTION	DESCRIPTION
Autoriser l'expéditeur pour tous les utilisateurs	Les expéditeurs des courriels sélectionnés sont autorisés pour tous les utilisateurs. Tous les courriels entrants des expéditeurs seront automatiquement distribués.
Courriel à admin	Les courriels sélectionnés sont envoyés à l'adresse courriel de la personne attribuée au contact **send_email_to_admin** sous **Tableau de bord des services** > **Gestion de rôles et contacts** (voir Attribuer un contact pour la distribution de courriels à la page 107).

REMARQUE :

Les expéditeurs interdits et autorisés sont traités comme suit :

- Expéditeurs interdits de l'administrateur
- Expéditeurs autorisés de l'administrateur
- Expéditeurs interdits de l'utilisateur
- Expéditeurs autorisés de l'utilisateur

Un administrateur interdit le compte example@example.com globalement. Un utilisateur autorise le même compte. Tous les courriels du compte sont distribués à l'utilisateur, tous les autres utilisateurs qui n'ont pas autorisé le compte eux-mêmes ne reçoivent pas de courriels.

Prévisualisation de courriel

La prévisualisation de courriel dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) permet aux utilisateurs et aux délégués d'afficher le contenu des courriels des catégories suivantes (voir Catégories de courriels à la page 84) :

- **Spam**

- **Threat**
- **AdvThreat**
- **Contenu**
- **Infomail**
- **Valide**

La prévisualisation de courriel est prise en charge par les navigateurs suivants dans la version actuelle :

- Edge
- Chrome
- Firefox
- Safari

La prévisualisation de courriel est accessible dans le module **Email Live Tracking** et dans les rapports de quarantaine (voir le chapitre « À propos du Quarantine Report » dans le manuel du Control Panel). Dans le module **Email Live Tracking**, la prévisualisation de courriel est disponible uniquement pour les courriels qui appartiennent à l'utilisateur ou qui appartenaient à une boîte aux lettres qui a été supprimée et attribuée à l'utilisateur à posteriori. Les délégués peuvent afficher une prévisualisation pour des courriels de la boîte aux lettres pour laquelle ils ont été enregistrés en tant que délégué (voir Saisir une délégation à la page 245). Pour de plus amples informations, voir Actions sur les courriels à la page 89. Dans les rapports de quarantaine, la prévisualisation de courriel est disponible uniquement si l'administrateur a opté pour une mise en page avec prévisualisation de courriel et s'il a généré des rapports de quarantaine propres pour chaque utilisateur du domaine (voir Configurer le Quarantine Report pour un domaine à la page 430).

La prévisualisation de courriel est accessible via un bouton dans le module **Email Live Tracking** et dans les rapports de quarantaine. Dès qu'un utilisateur accède à la prévisualisation de courriel, un service Web est appelé dans une nouvelle fenêtre du navigateur via un lien crypté.

Le lien crypté est valide uniquement pour un temps limité. Dans le module **Email Live Tracking**, le lien crypté est généré dès que l'utilisateur accède à la prévisualisation de courriel dans le module. Ce lien est valide une seule fois. L'utilisateur peut créer un nouveau lien dans le module aussi souvent qu'il le souhaite. Cette option est disponible pendant six mois par défaut. Les liens des rapports de

quarantaine sont valides 14 jours et peuvent être utilisés de manière illimitée pendant cette période. Les liens dans les rapports de quarantaine ne peuvent pas être générés à nouveau.

Le contenu du courriel sélectionné s'affiche de manière sécurisée dans le service Web. Les images du courriel sont remplacées par des caractères de remplacement sûrs avec le texte **Original image has been removed for security reasons.**. Les liens et autres contenus actifs sont désactivés. Si nécessaire et dans la mesure du possible, la mise en page et le codage du courriel sont légèrement modifiés pour afficher le contenu du courriel.

IMPORTANT :

La prévisualisation du courriel s'ouvre dans une fenêtre contextuelle. Il est possible que le navigateur bloque la fenêtre contextuelle. La fenêtre contextuelle peut être autorisée dans les paramètres du navigateur.

Illustration 75 : Prévisualisation d' un courriel

Les utilisateurs peuvent se faire remettre des courriels depuis la prévisualisation. Pour cela, les utilisateurs ont les options suivantes qu'ils peuvent déclencher en cliquant sur des boutons en haut de la prévisualisation :

- **Libérer le courriel** : Le courriel est remis. Pour de plus amples informations, voir l'explication de l'action sur le courriel **Libérer le courriel** sous Actions sur les courriels à la page 89.

  REMARQUE :

  Cette action n'est pas disponible pour les courriels qui sont adressés aux boîtes auxc lettres de renvoi (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel). Si les utilisateurs essaient d'exécuter cette action, ils recevront un message d'erreur.

- **Autoriser l'expéditeur et libérer le courriel** : L'expéditeur du courriel est autorisé pour l'utilisateur et le courriel est distribué. Tous les autres courriels de l'expéditeur seront automatiquement distribués.

  REMARQUE :

  Cette action n'est pas disponible pour les courriels qui sont adressés aux boîtes auxc lettres de renvoi (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel). Si les utilisateurs essaient d'exécuter cette action, ils recevront un message d'erreur.

- **Ne jamais afficher l' expéditeur** : L'expéditeur est mis sur la liste des expéditeurs interdits de l'utilisateur et les futurs courriels de cet expéditeur seront exclus des rapports de quarantaine (voir À propos du Quarantine Report à la page 418).

> **REMARQUE :**
>
> Ce bouton apparaît uniquement si l'option **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine** est activée pour les rapports de quarantaine (voir Configurer le Quarantine Report pour une boîte aux lettres à la page 436).

> **REMARQUE :**
>
> Cette action n'est pas disponible pour les courriels qui sont adressés aux boîtes auxc lettres de renvoi (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel). Si les utilisateurs essaient d'exécuter cette action, ils recevront un message d'erreur.

Exporter les données de courriels sous un fichier CSV

Vous pouvez exporter les résultats de recherche actuels du module **Email Live Tracking** (voir Email Live Tracking à la page 59) sous forme de fichier CSV. Les résultats de la recherche dépendent des filtres définis (voir Filtre de champ à la page 70). Les lignes dans le fichier d'exportation sont triées de la même façon que les données dans le module **Email Live Tracking**.

> **REMARQUE :**
>
> Si une période (**Le mois dernier**, **Cette année** etc.) est sélectionnée, le fuseau horaire UTC est utilisé par défaut, quels que soient les paramètres de l'utilisateur. Si un fuseau horaire autre que l'UTC est défini pour l'utilisateur, les données du dernier jour civil avant la période sélectionnée peuvent donc également être exportées.

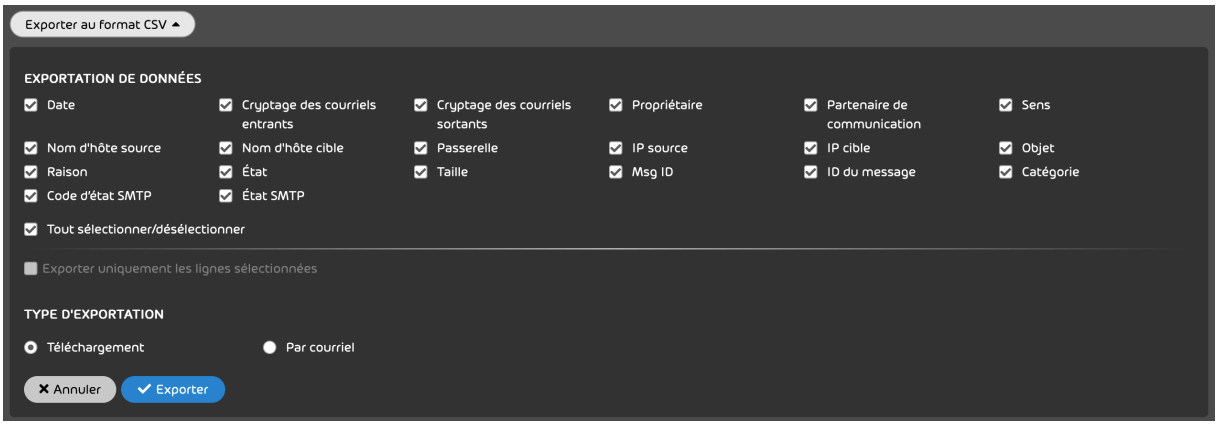
1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Facultatif : Si vous souhaitez accéder aux courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.

3. Naviguez vers le module **Email Live Tracking**
4. Facultatif : Si vous ne souhaitez exporter que certains courriels, filtrez les courriels affichés (voir Filtrer les courriels à la page 66).

Dans le module **Email Live Tracking**, seuls les courriels correspondant aux paramètres de recherche sont affichés.

5. Cliquez sur **Exporter au format CSV**.

Un sous-menu avec des paramètres avancés s'ouvre.



6. Sélectionnez les colonnes de tableau que vous souhaitez exporter.

> **REMARQUE :**
>
> Pour de plus amples informations sur les champs du courriel, voir Informations élargies des courriels à la page 79.

7. Sélectionnez le type d'exportation souhaité :
   - **Téléchargement**
   - **Par courriel**

8. Cliquez sur **Exporter** pour exporter les données de courriels des colonnes de tableau sélectionnées sous forme de fichier CSV.

> **REMARQUE :**
>
> Cette fonction permet d'exporter au maximum 10 000 entrées par fichier. Si les résultats de la recherche contiennent plus de 10 000 entrées, seules les 10 000 premières entrées seront exportées selon le tri actuel.

Les données de courriels ont été exportées sous forme de fichier CSV.

Tableau de bord des services

À propos du tableau de bord des services

Le tableau de bord des services propose aux administrateurs la possibilité de garder le contrôle sur les activités administratives.

Le tableau de bord des services montre une vue d'ensemble de tous les rôles créés des différents domaines d'utilisateurs

Dans la section **Gestion de rôles et contacts**, les administrateurs côté partenaires et clients peuvent créer de nouvelles attributions de rôle (voir Rôles à la page 49) et gérer les modifications de rôle existantes (voir Administration des rôles et contacts à la page 101). Par ailleurs, les administrateurs peuvent stocker les coordonnées de diverses instances de leur entreprise (voir Ajouter des coordonnées à la page 104).

Dans la section **Environnements secondaires**, les administrateurs côté clients peuvent gérer des environnements secondaires pour diriger le trafic de courriels entrants de certaines boîtes aux lettres d'un domaine vers un autre serveur de destination (voir Environnements secondaires à la page 113).

Dans l'onglet **Connexion LDAP**, les administrateurs côté clients peuvent également configurer la connexion LDAP dans le Control Panel (voir Connexion LDAP à la page 122).

En outre, les administrateurs côté partenaires et clients peuvent définir des valeurs par défaut pour le fuseau horaire, la langue, le format de date et le format d'heure pour tous leurs partenaires, clients et utilisateurs subordonnés dans l'onglet **Fuseau horaire et langue par défaut** (voir Régler les valeurs par défaut pour le fuseau horaire et la langue à la page 145).

En outre, les administrateurs côté partenaires peuvent définir un contrat de licence pour l'utilisateur final et un contrat de traitement des données dans l'onglet **Termes et conditions** (voir Conditions générales à la page 147) afin d'obtenir l'accord des utilisateurs de leurs clients concernant les conditions contractuelles.

Administration des rôles et contacts

Dans le module **Tableau de bord des services**, les administrateurs peuvent gérer les attributions de rôles de leurs utilisateurs ainsi que les contacts au sein de leur propre organisation. Les utilisateurs avec un rôle attribué ont d'autres autorisations en tant que simples utilisateurs (voir le chapitre « Rôles » dans le manuel du Control Panel). Les contacts sont les interlocuteurs d'une instance de l'organisation (voir Contacts à la page 102).

Dans **Gestion de rôles et contacts**, les actions suivantes peuvent être exécutées :

- Attribuer un rôle à un utilisateur (voir Attribuer un rôle à la page 103).
- Enregistrer un utilisateur en tant que contact (voir Ajouter des coordonnées à la page 104)
- Enregistrer un utilisateur comme contact pour la distribution de courriels (voir Attribuer un contact pour la distribution de courriels à la page 107)
- Filtrer les rôles et les contacts (voir Filtrer les rôles et les contacts à la page 108)
- Supprimer une attribution de rôle ou un contact (voir Supprimer une attribution de rôle ou un contact à la page 110)

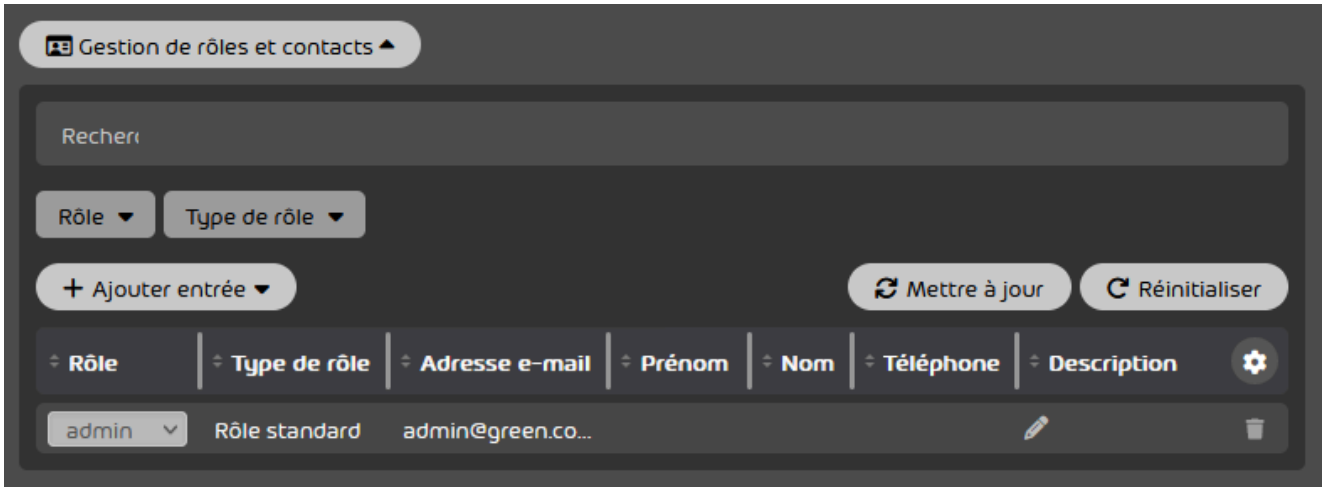


Illustration 76 : Vue d' ensemble de l' administration des rôles et contacts

Contacts

Les administrateurs côté clients et côté partenaires peuvent enregistrer des utilisateurs individuels comme contacts dans le Control Panel. Les contacts font référence aux instances au sein de l'organisation du client ou du partenaire. L'attribution de contacts permet aux administrateurs de voir à tout moment dans le Control Panel qui est l'interlocuteur pour une instance au sein d'une organisation.

Contrairement aux rôles (voir le chapitre « Rôles » dans le manuel du Control Panel), les contacts n'ont aucune influence sur les autorisations des utilisateurs dans le Control Panel. La plupart des contacts n'affectent pas non plus les fonctionnalités du Control Panel. Seul de contact **send_email_to_admin** est lié à une action au sein du Control Panel.

Les contacts sont expliqués dans le tableau suivant.

Tableau 9 : contacts

CONTACT	EXPLICATION
it_director	Direction du département de technologie de l'information
helpdesk	Collaborateurs du support technique
sales	Collaborateurs du département des ventes
license_management	Collaborateur responsable de la gestion des licences
emergency	Contact d'urgence
personal_contact	Contact personnel
send_email_to_admin	Collaborateurs auxquels des courriels devraient être envoyés via l'action **Courriel à admin** dans le module **Email Live Tracking**

Attribuer un rôle

Les utilisateurs avec un rôle attribué (voir Rôles à la page 49) ont d'autres autorisations en tant que simples utilisateurs. Dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous pouvez attribuer des rôles à vos utilisateurs afin de leur fournir des autorisations supplémentaires.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine de l'utilisateur à qui vous souhaitez attribuer un rôle.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Cliquez sur **Gestion de rôles et contacts** > **Ajouter entrée**.

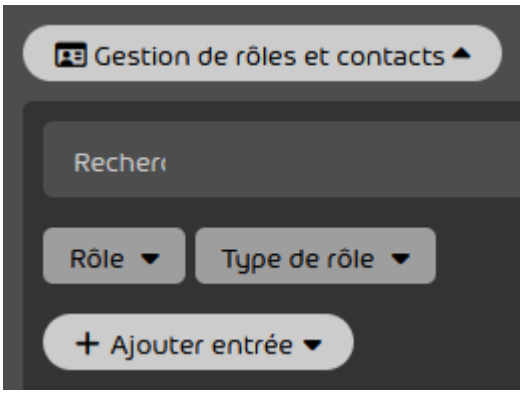


Illustration 77 : Ajouter une entrée

6. Saisissez sous **Sélectionner utilisateur** l'utilisateur auquel vous souhaitez attribuer un nouveau rôle.

7. Dans le menu déroulant, sélectionnez quel rôle vous souhaitez attribuer à l'utilisateur.

> **REMARQUE :**
>
> Pour une description des rôles, voir le chapitre Rôles à la page 49.

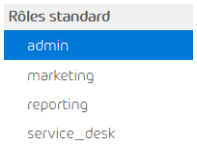


Illustration 78 : Sélection du rôle

8. Cliquez sur **Confirmer**.

Le rôle est attribué à l'utilisateur. L'utilisateur apparaît avec le rôle attribué dans le tableau.

Un rôle a été attribué à un utilisateur.

Ajouter des coordonnées

Dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous pouvez ajouter des coordonnées pour différentes instances de votre organisation en attribuant des utilisateurs comme contacts aux instances. Les coordonnées des utilisateurs attribués sont enregistrées pour les instances.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine au niveau duquel vous souhaitez enregistrer un utilisateur comme contact.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.

5. Cliquez sur **Gestion de rôles et contacts** > **Ajouter entrée**.

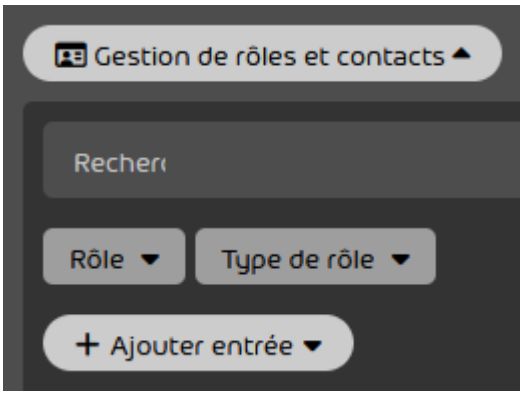


Illustration 79 : Ajouter une entrée

6. Dans le menu déroulant, sélectionnez une instance à laquelle vous souhaitez attribuer les coordonnées d'un utilisateur.

   Vous pouvez choisir parmi les instances suivantes :

   - it_director
   - helpdesk
   - sales
   - license_management
   - emergency
   - personal_contact
   - send_email_to_admin

   IMPORTANT :

   Le contact **send_email_to_admin** est différent du rôle **admin**. L'action **Courriel à admin** sous **Email Live Tracking** permet d'envoyer des courriels uniquement à la personne qui a été enregistrée pour le contact **send_email_to_admin** (voir Attribuer un contact pour la distribution de courriels à la page 107).

   REMARQUE :

   Pour de plus amples informations sur les contacts, voir Contacts à la page 102.

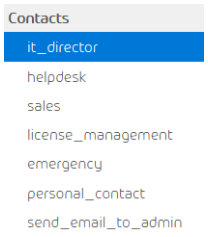


Illustration 80 : Sélectionner une instance

7. Sous **Sélectionner utilisateur**, sélectionnez un utilisateur dont vous voulez stocker les données comme coordonnées pour l'instance sélectionnée.

8. Cliquez sur **Confirmer**.

Les données de l'utilisateur sélectionné sont affectées à l'instance. L'entrée est affichée dans le tableau et est identifiée sous **Type de rôle** comme **Contact**.

Un utilisateur a été enregistré comme contact pour une instance.

Attribuer un contact pour la distribution de courriels

Vous pouvez attribuer le contact **send_email_to_admin** à un utilisateur afin que vos utilisateurs puissent envoyer des courriels aux utilisateurs affectés dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59). Si le contact **send_email_to_admin** est attribué à un utilisateur, les utilisateurs peuvent distribuer des courriels aux utilisateurs affectés, dans le module **Email Live Tracking** via l'action **Courriel à admin** (voir Actions sur les courriels à la page 89). Autrement, cette action de courriel ne sera pas disponible pour les utilisateurs du domaine et sera masquée dans le Control Panel.

REMARQUE :

Le contact **send_email_to_admin** est automatiquement attribué au premier administrateur qui a été défini pour un client. Toutefois, les administrateurs peuvent supprimer ce contact s'ils le souhaitent (voir Supprimer une attribution de rôle ou un contact à la page 110).

Vous pouvez attribuer le contact **send_email_to_admin** manuellement à un utilisateur.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Naviguez vers **Tableau de bord des services**.
3. Sélectionnez l'onglet **Administration**.
4. Cliquez sur **Gestion de rôles et contacts** > **Ajouter entrée**.

Un affichage étendu s'ouvre.

5. Dans le menu déroulant, sélectionnez le contact **send_email_to_admin**.

Illustration 81 : Sélectionner un contact

6. Sous **Sélectionner utilisateur**, saisissez l'utilisateur auquel vous souhaitez attribuer le contact.

Le bouton **Ajouter** est déverrouillé.

7. Cliquez sur **Ajouter**.

Le contact est attribué à l'utilisateur. L'attribution est ajoutée dans le tableau ci-dessous.

> **REMARQUE :**
>
> Si le contact **send_email_to_admin** n'était attribué à aucun utilisateur auparavant, les utilisateurs du domaine doivent se déconnecter une fois du Control Panel et se reconnecter pour que la modification soit enregistrée.

Le contact **send_email_to_admin** a été attribué à un utilisateur. Les utilisateurs peuvent dès à présent distribuer des courriels aux utilisateurs affectés, dans le module **Email Live Tracking** via l'action **Courriel à admin**.

Filtrer les rôles et les contacts

Vous avez attribué des rôles aux utilisateurs (voir Attribuer un rôle à la page 103) et enregistré des utilisateurs comme contacts (voir Ajouter des coordonnées à la page 104).

Dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous pouvez filtrer des rôles (voir Rôles à la page 49) et des contacts par rôle attribué ou par type de rôle afin de faciliter la gestion des rôles et des contacts.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine au niveau duquel vous souhaitez filtrer des rôles et des contacts.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Cliquez sur **Gestion de rôles et contacts**.
6. Filtrez par rôle ou par type de rôle :
   - Pour filtrer un rôle, sélectionnez le rôle dans le menu déroulant **Rôle**.
   - Pour filtrer par type de rôle, sélectionnez le type de rôle dans le menu déroulant **Type de rôle**.

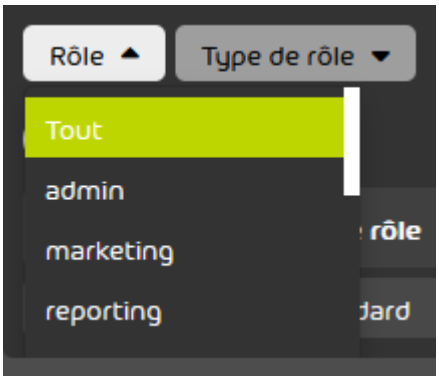


Illustration 82 : Filtrer par rôle

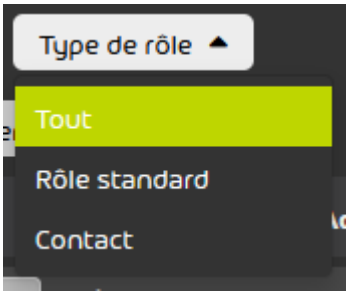


Illustration 83 : Filtrer par type de rôle

Les entrées filtrées sont affichées dans le tableau.

Les rôles et les contacts ont été filtrés.

Supprimer une attribution de rôle ou un contact

Vous avez attribué un rôle à un utilisateur (voir Attribuer un rôle à la page 103) ou vous avez enregistré un utilisateur comme contact (voir Ajouter des coordonnées à la page 104).

Dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), des rôles peuvent être attribués à des utilisateurs (voir Rôles à la page 49) et des utilisateurs peuvent être enregistrés comme contacts (voir Ajouter des coordonnées à la page 104). Les utilisateurs avec un rôle attribué ont d'autres autorisations en tant que simples utilisateurs. Les contacts sont les interlocuteurs d'une instance de l'entreprise. Si une attribution de rôles existante ou un contact existant n'est plus actuel, vous pouvez supprimer l'attribution de rôles ou le contact.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine des utilisateurs pour lesquels vous souhaitez supprimer une attribution de rôle ou un contact.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.

5.

IMPORTANT :

Si le dernier contact **send_email_to_admin** est supprimé, l'action sur les courriels **Courriel à admin** est masquée pour les utilisateurs du domaine dans le module **Email Live Tracking** et n'est plus disponible pour eux.

IMPORTANT :

Le rôle **admin** doit être attribué à au moins un utilisateur. Vous pouvez supprimer l'attribution du rôle à un utilisateur uniquement si le rôle est attribué à un autre utilisateur.

REMARQUE :

Les utilisateurs avec le rôle **admin** peuvent supprimer leur propre attribution au rôle **admin**.

Cliquez à droite sur la ligne de l'attribution de rôle ou du contact à supprimer sur .

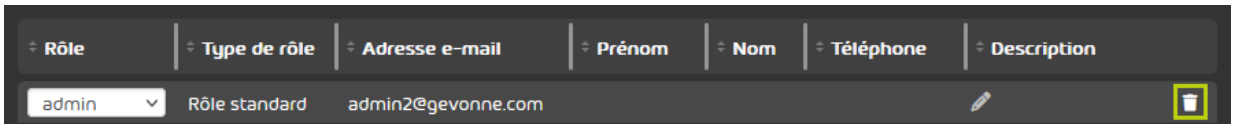


Illustration 84 : supprimer une entrée

Un message d'avertissement apparaît.

Illustration 85 : Avertissement

6. Confirmez la suppression de l'entrée avec **Confirmer**.

L'entrée est supprimée.

> **REMARQUE :**
>
> Si le dernier contact **send_email_to_admin** est supprimé, les utilisateurs du domaine doivent se déconnecter une fois du Control Panel et se connecter à nouveau pour que la modification soit effectuée.

Une attribution de rôle ou un contact a été supprimé.

Supprimer un client propre

Dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), en tant qu'administrateur côté client, vous pouvez supprimer du Control Panel les clients que vous administrez.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine du client que vous souhaitez supprimer.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Dans **Gestion de rôles et contacts**, cliquez sur **Supprimer le client sélectionné**.

Illustration 86 : Supprimer un client

Une fenêtre de confirmation s'ouvre.

6. Dans le champ de saisie, saisissez le nom du client que vous souhaitez supprimer.

Illustration 87 : Saisir le nom du client

7. Cliquez sur **Confirmer**

Le client est supprimé.

Un client a été supprimé du Control Panel.

Environnements secondaires

Par défaut, le trafic de courriels entrants de toutes les boîtes aux lettres d'un domaine est dirigé vers un serveur de destination défini dans le module **Spam and Malware Protection** (voir Procéder à la configuration de l'environnement principal à la page 457). Ce serveur de destination est désigné comme un environnement principal.

Il est possible de diriger le trafic de courriels entrants de certaines boîtes aux lettres vers d'autres serveurs de destination. Ces autres serveurs de destination sont désignés dans le Control Panel comme des environnements secondaires. On distingue plusieurs types d'environnements secondaires (voir Types d'environnements secondaires à la page 114). Dans le module **Tableau de bord des services**, les environnements secondaires peuvent être créés (voir Créer un environnement secondaire à la page 116), édités (voir Éditer l'environnement secondaire à la page 118) et supprimés (voir Supprimer un environnement secondaire à la page 120).

Types d’ environnements secondaires

Dans le Control Panel, des environnements secondaires peuvent être gérés en plus de l'environnement principal (voir « Configuration d'environnement principal » dans le manuel du Control Panel) vers lequel le trafic des courriels entrants des boîtes aux lettres d'un domaine est dirigé par défaut. Les environnements secondaires sont définis comme des serveurs de destination vers lesquels le trafic de courriels entrants de certaines boîtes aux lettres du domaine doit être acheminé au lieu de l'environnement principal. Les types d'environnements secondaires suivants sont gérés dans le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) :

- **Individuel** : les administrateurs peuvent définir des serveurs de destination propres avec ce type d'environnements secondaires. Ils peuvent ainsi définir les adresses IPv4 ou les noms d'hôtes des serveurs de destination. Les administrateurs peuvent créer plusieurs environnements de ce type.

Synchronisation des environnements secondaires

Les boîtes aux lettres synchronisées avec un service d'annuaire via LDAP sont attribuées par défaut à l'environnement principal dans le Control Panel (voir « Configuration d'environnement principal » dans le manuel du Control Panel). Contrairement aux boîtes aux lettres non synchronisées, les boîtes aux lettres synchronisées ne peuvent pas être manuellement attribuées à un environnement secondaire dans le Control Panel (voir Environnements secondaires à la page 113).

En revanche, il est possible d'attribuer automatiquement ces boîtes aux lettres à des environnements secondaires. Pour cela, la boîte aux lettres dans le service d'annuaire doit appartenir à un groupe dont le nom correspond au nom de l'environnement secondaire dans le Control Panel. Le fait que ce groupe existe ou non dans le Control Panel est sans importance.

Lors de la synchronisation d'une boîte aux lettres dans le Control Panel, les noms de ses groupes dans le service d'annuaire sont comparés l'un après l'autre aux noms des environnements secondaires. Dès qu'une correspondance est constatée, le traitement d'autres groupes est arrêté et la boîte aux lettres est attribuée à l'environnement secondaire. Les autres concordances ne sont donc pas prises en compte.

REMARQUE :

L'ordre dans lequel les groupes sont traités dépend du tableau Unicode. Les caractères suivants, par exemple, sont triés dans l'ordre suivant. La liste suivante ne contient toutefois que quelques caractères et ne saurait donc être exhaustive.

1. Point d'exclamation !
2. Losange #
3. Astérisque *
4. Signe plus +
5. Signe moins -
6. Chiffres
7. Signe inférieur à <
8. Signe supérieur à >
9. Tiret bas _
10. Minuscule
11. Tilde ~
12. Voyelles infléchies dans les minuscules

Toutes les lettres dans les noms des groupes et des environnements secondaires sont traitées comme des minuscules.

Pour qu'une boîte aux lettres synchronisée soit attribuée au bon environnement secondaire, nous recommandons de procéder comme suit : L'administrateur attribue la boîte aux lettres dans le service d'annuaire à un groupe précis dont le nom correspond au nom d'un environnement secondaire dans le Control Panel. Il s'agit de l'environnement secondaire auquel la boîte aux lettres doit être attribuée.

IMPORTANT :

Pour qu'une boîte aux lettres synchronisée soit attribuée à l'environnement principal, celle-ci ne doit appartenir à aucun groupe dans le service d'annuaire dont le nom correspond à celui d'un environnement secondaire dans le Control Panel.

Créer un environnement secondaire

Par défaut, le trafic de courriels entrants de toutes les boîtes aux lettres d'un domaine est dirigé vers un serveur de destination défini dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450) comme environnement principal (voir Procéder à la configuration de l'environnement principal à la page 457). Si le trafic de courriels de certaines boîtes aux lettres du domaine doit être dirigé vers d'autres serveurs de destination, vous pouvez créer des environnements secondaires pour ces serveurs de destination.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer un environnement secondaire.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Dans **Environnements secondaires**, cliquez sur **Ajouter environnement secondaire**.

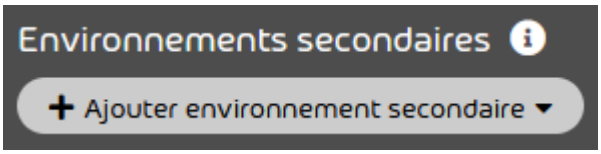


Illustration 88 : Ajouter un environnement secondaire

Un menu s'ouvre.

6. Sélectionnez l'onglet correspondant au type d'environnement secondaire que vous souhaitez créer (voir Types d'environnements secondaires à la page 114). Vous pouvez choisir parmi les types d'environnements secondaires suivants :

   - **Individuel**

7. **IMPORTANT :**

   Les les boîtes aux lettres LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel) sont automatiquement attribuées à un environnement secondaire pendant la synchronisation dans le Control Panel dans la mesure où les boîtes aux lettres sont attribuées dans le service d'annuaire à un groupe dont le nom correspond à un environnement secondaire dans le Control Panel. Les boîtes aux lettres sont attribuées à l'environnement secondaire du même nom.

   Les noms des groupes sont traités l'un après l'autre conformément au tableau Unicode et comparés aux noms des environnements secondaires. La boîte aux lettres est attribuée au premier environnement secondaire pour lequel une correspondance est constatée. Pour de plus amples informations, voir Synchronisation des environnements secondaires à la page 114.

   Dans le champ **Nom de l'environnement dans le Control Panel**, saisissez le nom sous lequel doit s'afficher l'environnement secondaire dans le Control Panel.

Illustration 89 : Saisir les noms de l'environnement secondaire

8. Facultatif : Si vous avez sélectionné l'onglet **Individuel**, dans le champ **Adresse du serveur de destination**, saisissez l'adresse IPv4 ou le nom d'hôte du serveur de destination.

Illustration 90 : Saisir l'adresse du serveur de destination

9. Cliquez sur **Ajouter**.

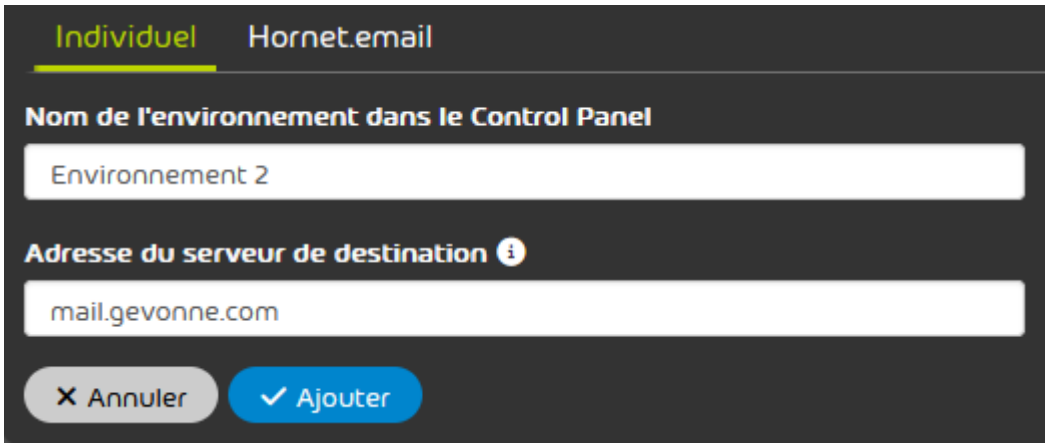


Illustration 91 : Ajouter un environnement secondaire

L'environnement secondaire est créé et ajouté à l'onglet sous **Environnements secondaires**.

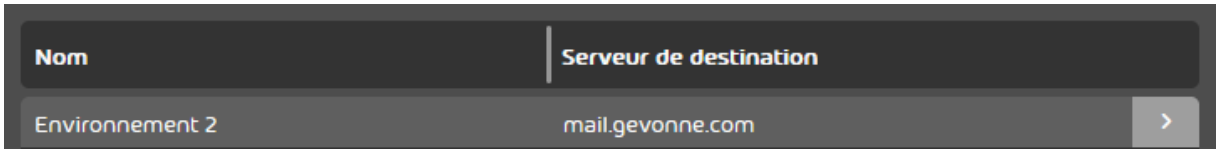


Illustration 92 : Liste des environnements secondaires

Un environnement secondaire a été créé.

Vous pouvez ensuite attribuer l'environnement secondaire à des boîtes aux lettres de votre domaine (voir Modifier l'environnement à la page 257). Si vous n'avez plus besoin de l'environnement secondaire, vous pouvez le supprimer (voir Supprimer un environnement secondaire à la page 120).

Éditer l'environnement secondaire

Vous avez créé un environnement secondaire (voir Créer un environnement secondaire à la page 116).

Vous pouvez éditer des environnements secondaires existants. Toutefois, vous ne pouvez pas modifier le type d'environnement secondaire (voir Types d' environnements secondaires à la page 114).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez éditer un environnement secondaire existant.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Dans la liste sous **Environnements secondaires**, sélectionnez l'environnement secondaire et cliquez sur la flèche du menu à côté de l'environnement secondaire.

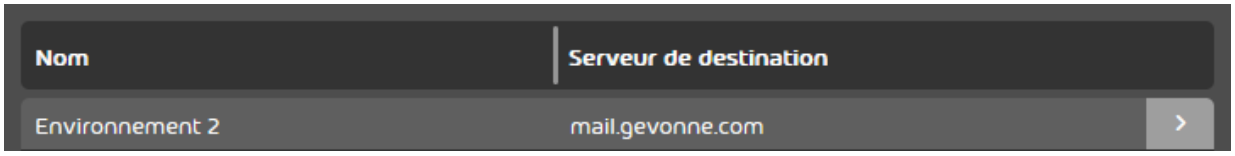


Illustration 93 : Ouvrir le menu

- Un menu s'ouvre.

6. Cliquez sur **Éditer entrée**.

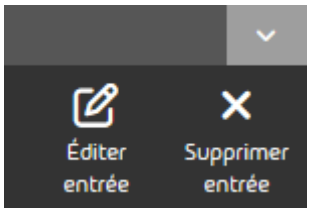


Illustration 94 : Éditer l' entrée

- Un menu avec les paramètres actuels de l'environnement secondaire s'ouvre.

7. Éditez les paramètres de l'environnement secondaire en fonction de vos souhaits (voir Créer un environnement secondaire à la page 116).

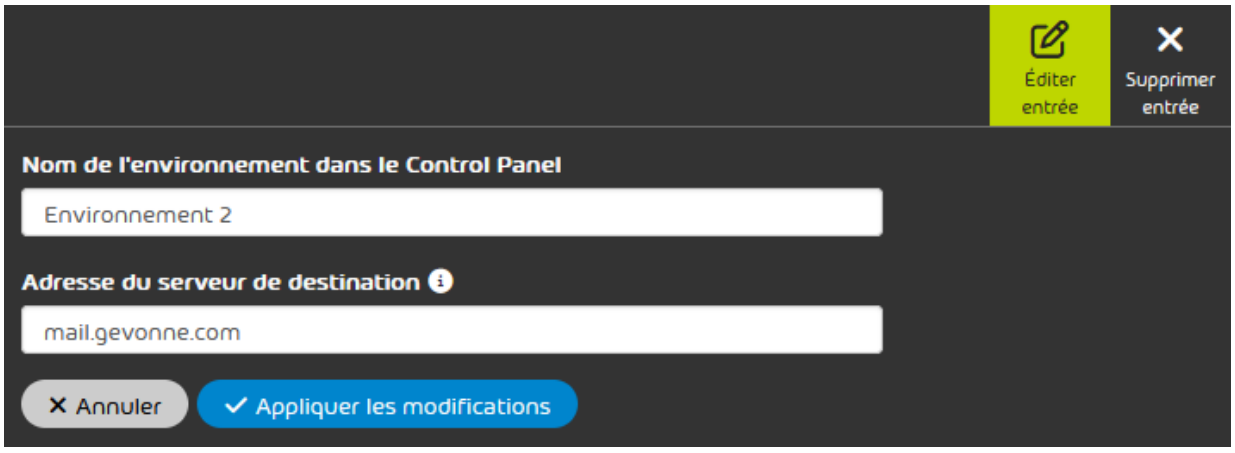


Illustration 95 : Éditer l' environnement secondaire

8. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées et appliquées à toutes les boîtes aux lettres auxquelles est attribué l'environnement secondaire.

Un environnement secondaire existant a été édité.

Supprimer un environnement secondaire

Vous avez créé un environnement secondaire (voir Créer un environnement secondaire à la page 116).

Si vous n'avez plus besoin d'un environnement secondaire, vous pouvez le supprimer. Dès que vous supprimez un environnement secondaire, les boîtes aux lettres auxquelles l'environnement secondaire a été attribué, se voient attribuer l'environnement principal à la place (voir Configuration d' environnement principal à la page 456).

IMPORTANT :

Si les boîtes aux lettres de l'environnement primaire sont synchronisées avec un service d'annuaire via LDAP, les boîtes aux lettres de l'environnement secondaire supprimé seront attribuées à l'environnement primaire, mais elles ne seront pas synchronisées.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer un environnement secondaire.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Administration**.
5. Dans la liste sous **Environnements secondaires**, sélectionnez l'environnement secondaire et cliquez sur la flèche du menu à côté de l'environnement secondaire.

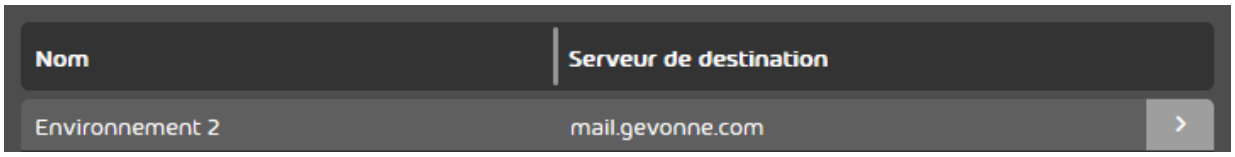


Illustration 96 : Ouvrir le menu

- Un menu s'ouvre.

6. Cliquez sur **Supprimer entrée**.

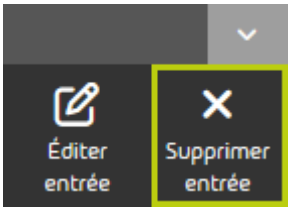


Illustration 97 : Supprimer l' entrée

- Un message apparaît.

7. Cliquez sur **Confirmer**.

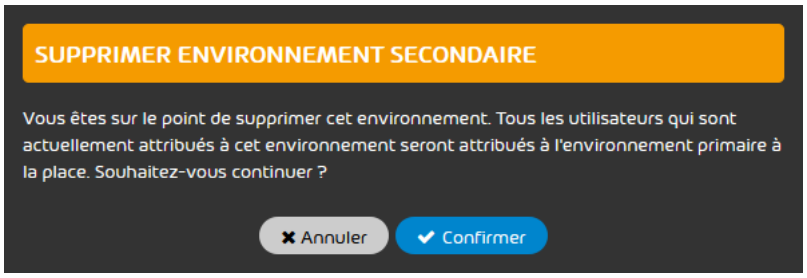


Illustration 98 : Supprimer un environnement secondaire

L'environnement secondaire est supprimé. Les boîtes aux lettres auxquelles l'environnement secondaire a été attribué se voient attribuer l'environnement principal à la place.

Un environnement secondaire a été supprimé.

Connexion LDAP

Dans l'onglet **Connexion LDAP** du module **Tableau de bord des services**, les administrateurs côté clients peuvent connecter un service d'annuaire, par ex. Microsoft Active Directory (AD), au Control Panel via LDAP. La connexion LDAP ne peut être appliquée qu'à l'environnement primaire (voir le chapitre « Configuration d'environnement principal » dans le manuel du Control Panel).

Pour lier un service d'annuaire au Control Panel, les administrateurs côté clients doivent d'abord configurer les attributs LDAP du service d'annuaire dans le Control Panel (voir Configurer les attributs LDAP à la page 123). Les administrateurs peuvent ensuite ajouter une connexion LDAP (voir Ajouter une connexion LDAP à la page 125). Cela permet d'établir une connexion entre le Control Panel et un service d'annuaire. Il est possible d'ajouter plusieurs connexions LDAP pour différents services d'annuaire. Lors de l'ajout d'une connexion LDAP, les administrateurs peuvent également sécuriser la connexion LDAP en définissant LDAPS comme protocole d'accès. Comme mesure de protection supplémentaire, les administrateurs peuvent limiter l'accès à leur service d'annuaire à notre plage d'adresses IP (voir Limiter le service d'annuaire à notre plage d'adresses à la page 134). En outre, les administrateurs peuvent déterminer si les

utilisateurs et les groupes du service d'annuaire doivent être synchronisés dans le Control Panel. Les administrateurs peuvent vérifier le résultat de la synchronisation en affichant une liste des utilisateurs et des groupes à synchroniser.

Dès qu'il existe au moins une connexion LDAP active, les administrateurs côté clients peuvent faire en sorte que les utilisateurs puissent se connecter au Control Panel avec leurs identifiants du service d'annuaire (voir Configurer une connexion dans le Control Panel via LDAP à la page 135). Les administrateurs peuvent, grâce à une fonction de test, vérifier si la connexion est effectivement possible avec les identifiants du service d'annuaire.

Les administrateurs côté clients peuvent éditer des connexions LDAP par la suite (voir Éditer une connexion LDAP à la page 139). Si une connexion LDAP ne doit pas être utilisée temporairement, les administrateurs peuvent la désactiver (voir Désactiver la connexion LDAP à la page 140). Si une connexion LDAP n'est plus nécessaire, les administrateurs peuvent la supprimer (voir Supprimer une connexion LDAP à la page 143).

Configurer les attributs LDAP

Dans l'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir le chapitre « À propos du tableau de bord des services » dans le manuel du Control Panel), les attributs LDAP sont prédéfinis avec des valeurs standard pour le Microsoft Active Directory. Si les attributs réels de votre répertoire portent une autre désignation, vous pouvez les modifier sous **Attributs LDAP**. Les attributs LDAP s'appliquent à toutes les connexions LDAP du client dans le Control Panel (voir Ajouter une connexion LDAP à la page 125).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez configurer les attributs LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.

5. Remplissez le formulaire sous **Attributs LDAP**. Les champs ont les significations suivantes :

   - **Adresse e-mail** : attribut du service de répertoire sous lequel les adresses courriel des utilisateurs sont enregistrés. Dans un Microsoft Active Directory, l'attribut **proxyAddresses** est utilisé pour cela par défaut.
   - **Adresses e-mail alias** : attribut du service de répertoire sous lequel les adresses courriel d'alias des utilisateurs sont enregistrés. Dans un Microsoft Active Directory, l'attribut **proxyAddresses** est également utilisé pour cela par défaut.
   - **Groupe** : attribut du service de répertoire sous lequel sont indiqués les groupes. Dans un Microsoft Active Directory, l'attribut **memberOf** est utilisé pour cela par défaut.
   - **Nom de compte SAM** : attribut du service de répertoire sous lequel est saisi le nom du compte SAM. Dans un Microsoft Active Directory, l'attribut **sAMAccountname** est utilisé pour cela par défaut.
   - **Nombre minimal d'utilisateurs** : nombre d'utilisateurs minimal prévu pour la synchronisation LDAP. Cette valeur fait référence au nombre total d'utilisateurs synchronisés de toutes les connexions LDAP actives. Cette valeur peut être une valeur indicative pour la qualité de la synchronisation. Si cette valeur n'est pas atteinte lors d'une opération de synchronisation, un courriel est envoyé à l'adresse courriel indiquée sous **Adresse e-mail pour des notifications** indiquant les éventuels problèmes de synchronisation. La valeur prédéfinie est **1**.
   - **Nombre minimal de groupes** : de la même manière que **Nombre minimal d'utilisateurs**, mais pour les groupes au lieu des utilisateurs. La valeur prédéfinie est **0**.
   - **Adresse e-mail pour des notifications** : adresse courriel à laquelle les notifications de synchronisation LDAP doivent être envoyées.
   - **ID objet** : attribut du service de répertoire utilisé pour l'identification externe claire des boîtes aux lettres. Dans un Microsoft Active Directory, l'attribut **objectguid** est utilisé pour cela par défaut.
   - **Positions et langues pour le Security Awareness Service** : Attribut personnalisé du service d'annuaire, qui contient les positions et les langues des utilisateurs pour le Security

Awareness Service (voir Synchroniser la position et la langue pour le Security Awareness Service). L'attribut souhaité peut être sélectionné à partir d'un menu déroulant.

REMARQUE :

Ce champ est visible uniquement si le Security Awareness Service (voir À propos de Security Awareness Service) est activé.

Illustration 99 : Remplir le formulaire

6. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées.

Les attributs LDAP du service d'annuaire d'un client ont été configurés dans le Control Panel.

Vous pouvez ensuite ajouter une connexion LDAP au Control Panel (voir Ajouter une connexion LDAP à la page 125).

Ajouter une connexion LDAP

Vous avez configuré les attributs LDAP de votre service d'annuaire dans le Control Panel (voir Configurer les attributs LDAP à la page 123).

L'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir le chapitre « À propos du tableau de bord des services » dans le manuel du Control Panel) vous permet d'ajouter une connexion LDAP au Control Panel. Cela permet d'établir une

connexion entre le Control Panel et un service d'annuaire. Vous pouvez configurer la synchronisation des utilisateurs et des groupes à partir du service d'annuaire dans le Control Panel. Vous pouvez ajouter plusieurs connexions LDAP pour différents services d'annuaire au Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez ajouter une connexion LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Dans **Connexions LDAP disponibles**, cliquez sur **Ajouter une connexion LDAP**.

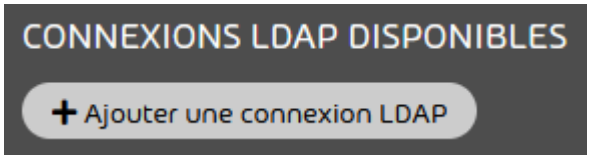


Illustration 100 : Ajouter une connexion LDAP

Un affichage étendu s'ouvre.

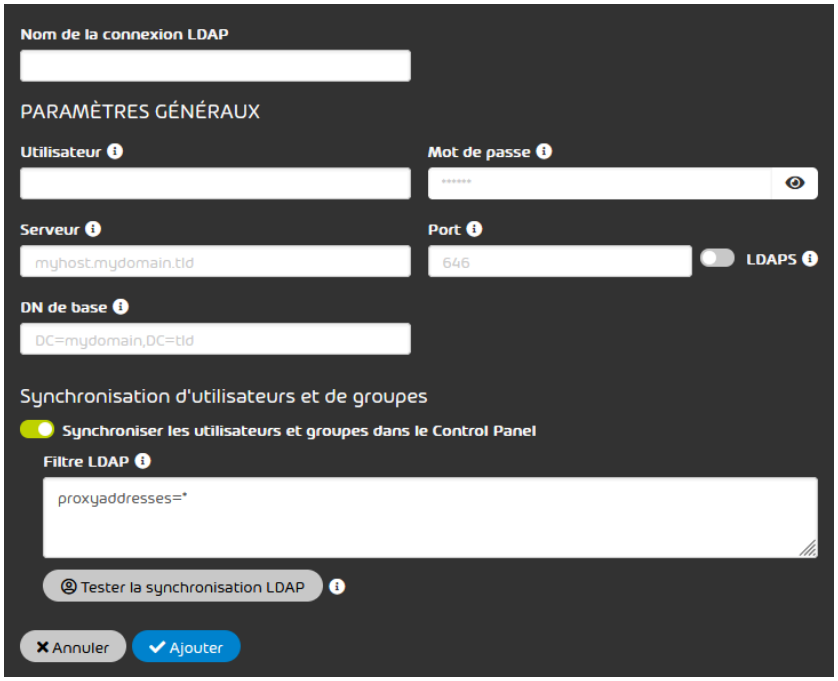


Illustration 101 : Vue élargie

6. Dans le champ **Nom de la connexion LDAP**, saisissez un nom pour la connexion LDAP.

7. Remplissez les champs sous **Paramètres généraux**. Les champs ont les significations suivantes :

   - **Utilisateur** : identifiant d'un utilisateur LDAP disposant des droits d'accès en lecture sur la structure de répertoire sous le DN de base. Il est également possible de saisir l'adresse courriel ou le chemin LDAP de l'utilisateur.

     REMARQUE :

     Dans le Microsoft Active Directory, les droits nécessaires sont délivrés à l'utilisateur par l'affectation au groupe **RAS and IAS Servers**.

     REMARQUE :

   - **Mot de passe** : Mot de passe de l'utilisateur
   - **Serveur** : Adresse IPv4 ou nom d'hôte du serveur de destination du service d'annuaire
   - **Port** : Port du serveur de destination du service d'annuaire. Les ports par défaut pour les différents protocoles LDAP sont :
     - LDAP : port 389
     - LDAPS : port 636
     - GC_LDAP : port 3268
     - GC_LDAPS : port 3269
   - **DN de base** : le chemin de base LDAP où l'utilisateur peut être trouvé. Par exemple : **DC=myDomain,DC=tld**.

8. Facultatif : Si votre service d'annuaire est accessible via le protocole LDAPS, appuyez sur le bouton **LDAPS**.

> **REMARQUE :**
>
> Le protocole LDAPS sécurise la connexion LDAP avec TLS/SSL. La connexion LDAP peut également être protégée en limitant le service d'annuaire à notre plage d'adresses IP (voir Limiter le service d'annuaire à notre plage d'adresses à la page 134).

Le bouton devient vert.

9. Facultatif : Si les utilisateurs et les groupes du service d'annuaire ne doivent pas être synchronisés dans le Control Panel, appuyez sur le bouton **Synchroniser les utilisateurs et groupes dans le Control Panel**.

REMARQUE :

La synchronisation des utilisateurs et des groupes est activée par défaut.

La synchronisation des utilisateurs et des groupes permet de transférer les utilisateurs et leurs appartenances à des groupes du service d'annuaire vers le Control Panel. Si les utilisateurs ou les appartenances à des groupes sont supprimés ou modifiés dans le service d'annuaire, ces modifications sont également appliquées dans le Control Panel.

Les boîtes aux lettres qui ont été créées manuellement dans le Control Panel ou proviennent d'autres sources que LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel) restent dans le Control Panel lors de la synchronisation avec LDAP. Lors de la synchronisation, seules les boîtes aux lettres créées au préalable via la synchronisation LDAP dans le Control Panel sont supprimées du Control Panel, mais ne sont alors plus présentes dans le service de répertoire.

REMARQUE :

L'appartenance aux groupes des boîtes aux lettres LDAP est gérée exclusivement dans le service d'annuaire. Par conséquent, il n'est pas possible d'ajouter ou de supprimer manuellement des boîtes aux lettres LDAP des groupes dans le Control Panel. Pour que les utilisateurs puissent être attribués aux groupes du service d'annuaire dans le Control Panel, des groupes portant le même nom doivent être créés manuellement dans le Control Panel. Pour de plus amples informations sur la création de groupes, voir « Groupes » dans le manuel du Control Panel. Il est cependant possible d'ajouter ou d'importer des boîtes aux lettres d'environnements secondaires dans des groupes qui sont synchronisés avec un service d'annuaire dans le Control Panel (voir « Gérer les membres » et « Importer des membres de groupe à partir d'un fichier CSV » dans le manuel du Control Panel).

REMARQUE :

Avec la synchronisation des utilisateurs du service d'annuaire, les adresses alias peuvent être attribuées automatiquement. Ceci a l'avantage qu'un seul rapport de quarantaine (voir « À propos du Quarantine Report » dans le manuel du Control Panel) est envoyé pour chaque adresse primaire, y compris toutes les adresses alias associées.

Le bouton devient gris. Le champ **Filtre LDAP** est masqué.

10. Si la synchronisation des utilisateurs et des groupes est activée, saisissez dans le champ **Filtre LDAP** le filtre LDAP utilisé pour trouver les utilisateurs et les groupes dans le service d'annuaire.

> **REMARQUE :**
>
> Le filtre LDAP **proxyaddresses=*** est préréglé. Ce filtre LDAP permet de trouver par défaut les utilisateurs et les groupes dans Microsoft Active Directory.

> **REMARQUE :**
>
> Si le filtre doit être modifié, la syntaxe suivante doit être employée :
>
> **(|(xxxxxxxxxx=xxxxxxxxxx)(xxxxxxxxxx=xxxxxxxxxx))**
>
> L'ensemble du filtre ainsi que chaque paire attribut-valeur doivent être entre parenthèses. Le **|** en préfixe introduit une relation OU entre les paramètres entre les parenthèses suivantes. Cela signifie qu'une seule des conditions enregistrées doit s'appliquer. Un lien ET entre les paramètres peut être établi par un **&** en préfixe.
>
> Il doit également y avoir au moins une entrée entre parenthèses.

> **REMARQUE :**
>
> L'expression **(|(sAMAccountType=805306368)(sAMAccountType=268435456)(sAMAccountType=268435457)(objectclass=publicFolder))** permet de trouver tous les utilisateurs depuis un Microsoft Active Directory.

11. Facultatif : Procédez comme suit si vous souhaitez vérifier quels utilisateurs et groupes à synchroniser sont trouvés dans le service d'annuaire avec le filtre LDAP saisi.

a) Cliquez sur **Tester la synchronisation LDAP**.

La fenêtre **Essai LDAP** s'ouvre.

Illustration 102 : Test LDAP

b) Dans le menu déroulant, sélectionnez l'option pour laquelle vous souhaitez afficher des informations supplémentaires. Vous pouvez choisir parmi les options suivantes.

- **Utilisateurs** : Les utilisateurs qui ont été trouvés dans le service d'annuaire avec le filtre LDAP et qui peuvent être synchronisés sont affichés.
- **Groupes** : Les groupes qui ont été trouvés dans le service d'annuaire avec le filtre LDAP et qui peuvent être synchronisés sont affichés.
- **Rapport** : Le protocole du test LDAP apparaît.

c) Vérifiez si les données affichées répondent à vos attentes quant au contenu de votre service d'annuaire.

d) Cliquez sur **Fermer**.

La fenêtre se ferme.

12. Cliquez sur **Appliquer les modifications**.

Les paramètres sont mémorisés. La connexion LDAP est ajoutée au Control Panel et activée.

REMARQUE :

La synchronisation des données à partir du service d'annuaire a lieu dans une cadence horaire. Il se peut donc que le résultat des paramètres n'apparaîsse pas avant deux heures.

Une connexion LDAP a été ajoutée au Control Panel. Si la synchronisation des utilisateurs et des groupes est activée, les utilisateurs et les groupes du service d'annuaire sont régulièrement synchronisés dans le Control Panel. Les utilisateurs synchronisés sont ajoutés au Control Panel en tant que boîtes aux lettres LDAP (voir le chapitre «#Types de boîtes aux lettres#» dans le manuel du Control Panel).

Vous pouvez ensuite configurer l'utilisation des identifiants du service d'annuaire pour la connexion au Control Panel des utilisateurs de boîtes aux lettres LDAP (voir Configurer une connexion dans le Control Panel via LDAP à la page 135). Vous pouvez modifier une connexion LDAP existante a posteriori (voir Éditer une connexion LDAP à la page 139). Vous pouvez également désactiver temporairement une connexion LDAP (voir Désactiver la connexion LDAP à la page 140) ou la supprimer du Control Panel (voir Supprimer une connexion LDAP à la page 143).

Limiter le service d'annuaire à notre plage d'adresses

Vous pouvez limiter l'accès à votre service d'annuaire (voir Connexion LDAP à la page 122) à notre plage d'adresses IP. La saisie de nos plages d'adresses IP dans le pare-feu de votre service d'annuaire vous permet d'éviter que les demandes des autres adresses IP soient acceptées par votre service d'annuaire.

Saisissez les plages d'adresses IP suivantes dans le pare-feu de votre service d'annuaire :

- 1ère plage : **83.246.65.0/24** avec masque de sous-réseau **255.255.255.0**, correspond à 83.246.65.1 à 83.246.65.255.
- 2e plage : **94.100.128.0/20** avec masque de sous-réseau **255.255.240.0**, correspond à 94.100.128.1 à 94.100.143.255.
- 3e plage : **185.140.204.0/22** avec masque de sous-réseau **255.255.252.0**, correspond à 185.140.204.1 à 185.140.207.255.

- 4e plage : **173.45.18.0/24** avec masque de sous-réseau **255.255.255.0**, correspond à 173.45.18.1 à 173.45.18.255.

REMARQUE :

Les clients du Canada doivent également saisir les domaines IP suivants :

- 5e plage : **108.163.133.224/27** avec masque de sous-réseau **255.255.255.224**, correspond à 108.163.133.224 à 108.163.133.255.
- 6e plage : **199.27.221.64/27** avec masque de sous-réseau **255.255.255.224**, correspond à 199.27.221.64 à 199.27.221.95.
- 7e plage : **209.172.38.64/27** avec masque de sous-réseau **255.255.255.224**, correspond à 209.172.38.64 à 209.172.38.95.
- 8e plage : **216.46.2.48/29** avec masque de sous-réseau **255.255.255.248**, correspond à 216.46.2.48 à 216.46.2.55.
- 9e plage : **216.46.11.224/27** avec masque de sous-réseau **255.255.255.224**, correspond à 216.46.11.224 à 216.46.11.255.

La plage d'adresses IP admissible dans votre pare-feu a été limitée à notre plage d'adresses IP.

Configurer une connexion dans le Control Panel via LDAP

Vous avez ajouté une connexion LDAP dans le Control Panel (voir Ajouter une connexion LDAP à la page 125).

L'onglet **Connexion LDAP** du module **Tableau de bord des services** vous permet de configurer que les utilisateurs de boîtes aux lettres LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel) doivent utiliser les identifiants du service d'annuaire pour se connecter au Control Panel.

REMARQUE :

La connexion avec les identifiants du service d'annuaire est possible pour les utilisateurs de toutes les connexions LDAP actives.

REMARQUE :

Si les données d'accès du service d'annuaire sont utilisées pour la connexion au Control Panel, les utilisateurs ne peuvent pas modifier leur mot de passe dans le Control Panel (voir le chapitre « Modifier le mot de passe » dans le manuel du Control Panel).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour les utilisateurs duquel vous souhaitez activer l'authentification avec les données d'accès du service d'annuaire.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Actionnez le bouton **Autentification dans le Control Panel avec des identifiants LDAP** sous **Connexion au Control Panel**.

Le champ supplémentaire **Filtre LDAP** s'affiche sous le bouton.

Illustration 103 : Filtre LDAP pour la connexion au Control Panel

6. Dans le champ **Filtre LDAP**, saisissez un filtre pour les utilisateurs ou les groupes du service d'annuaire qui doivent utiliser les identifiants du service d'annuaire pour se connecter au Control Panel.

> **REMARQUE :**
>
> Le filtre LDAP **proxyaddresses=*** est préconfiguré. Cette expression permet de sélectionner tous les utilisateurs d'un Microsoft Active Directory.

7. Si vous souhaitez vérifier si la connexion au Control Panel fonctionne avec des identifiants du service d'annuaire, procédez comme suit.

   a) Cliquez sur **Essayer connexion**.

La fenêtre **Essai de connexion LDAP** s'ouvre.

Illustration 104 : Essai de connexion LDAP

b) Dans le champ **Utilisateur**, saisissez l'adresse courriel de l'utilisateur pour lequel vous souhaitez tester la connexion au Control Panel.

c) Dans le champ **Mot de passe**, saisissez le mot de passe de l'utilisateur dans le service d'annuaire.

d) Cliquez sur **Confirmer**.

- Le contrôle est effectué et le résultat apparaît en bas de la fenêtre.

e) Cliquez sur **Fermer**.

- La fenêtre se ferme.

8. Cliquez sur **Appliquer les modifications**.

- Les modifications sont enregistrées.

> **REMARQUE :**
>
> La synchronisation des données à partir du service d'annuaire a lieu dans une cadence horaire. Pour cette raison, le résultat de vos paramètres peut ne pas apparaître avant deux heures, dans certaines conditions.

La connexion au Control Panel avec les identifiants du service d'annuaire a été configurée.

IMPORTANT :

La connexion via LDAP n'est valable que pour les utilisateurs qui disposent de boîtes aux lettres LDAP (voir le chapitre «#Types de boîtes aux lettres#» dans le manuel du Control Panel). Les utilisateurs qui disposent de boîtes aux lettres provenant d'un environnement secondaire peuvent continuer à se connecter avec leurs données d'accès gérées dans le Control Panel.

Éditer une connexion LDAP

Vous avez ajouté une connexion LDAP au Control Panel (voir Ajouter une connexion LDAP à la page 125).

L'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet d'éditer une connexion LDAP existante.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez modifier la connexion LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Sous **Connexions LDAP disponibles**, sélectionnez la connexion LDAP que vous souhaitez éditer et cliquez sur la flèche de menu à côté de la connexion LDAP.

Illustration 105 : Ouvrir le menu

Un menu s'ouvre.

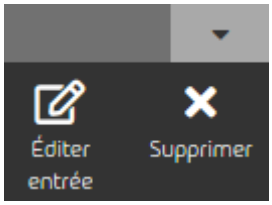


Illustration 106 : Menu

6. Cliquez sur **Éditer entrée**.

Les paramètres de la connexion LDAP sont affichés.

7. Modifiez les paramètres en fonction de vos souhaits (voir Ajouter une connexion LDAP à la page 125).
8. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> La synchronisation des données à partir du service d'annuaire a lieu dans une cadence horaire. Il se peut donc que le résultat des paramètres n'apparaîsse pas avant deux heures.

Une connexion LDAP existante a été éditée.

Désactiver la connexion LDAP

Vous avez ajouté une connexion LDAP dans le Control Panel (voir Ajouter une connexion LDAP à la page 125).

L'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet de désactiver une connexion LDAP existante si vous ne souhaitez plus synchroniser les utilisateurs et les appartenances à des groupes à partir du service d'annuaire dans le Control Panel. Si les utilisateurs ont préalablement utilisé leurs identifiants du service d'annuaire pour se connecter au Control Panel, le dernier mot de passe synchronisé reste enregistré dans le Control Panel et les utilisateurs peuvent

modifier leur mot de passe dans le Control Panel. Les paramètres sont conservés au cas où vous voudriez réactiver la connexion LDAP ultérieurement.

REMARQUE :

Après avoir désactivé la connexion LDAP, les données des utilisateurs dans le Control Panel ne sont plus synchronisées avec le service d'annuaire. Dès que les données du service d'annuaire changent, l'ensemble de données du Control Panel et l'ensemble de données du service d'annuaire diffèrent l'un de l'autre. Par exemple, les mots de passe ne sont plus renouvelés automatiquement dans le Control Panel, les boîtes aux lettres des nouveaux utilisateurs sont ajoutées au Control Panel à partir du service d'annuaire ou les boîtes aux lettres des utilisateurs supprimés sont supprimées du Control Panel.

Les boîtes aux lettres du Control Panel dont les données ont été préalablement synchronisées via LDAP continuent toutefois d'être protégées par nos services et sont toujours considérées comme des boîtes aux lettres LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez désactiver la connexion LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Sous **Connexions LDAP disponibles**, sélectionnez la connexion LDAP que vous souhaitez désactiver, puis cliquez sur la flèche de menu à côté de la connexion LDAP.

Illustration 107 : Ouvrir le menu

Un menu s'ouvre.

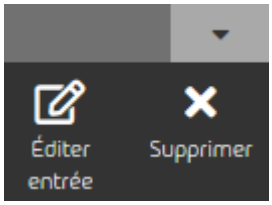


Illustration 108 : Menu

6. Cliquez sur **Éditer entrée**.

Les paramètres de la connexion LDAP sont affichés.

7. Actionnez le bouton **Activer connexion LDAP**.

Illustration 109 : Désactiver la connexion LDAP

Le bouton devient gris. Le bouton **Tester la synchronisation LDAP** sous **Synchronisation d'utilisateurs et de groupes** est bloqué.

8. Cliquez sur **Appliquer les modifications**.

Les paramètres sont mémorisés.

Une connexion LDAP a été désactivée.

Activer la connexion LDAP

Vous avez désactivé une connexion LDAP existante (voir Désactiver la connexion LDAP à la page 140).

Dans l'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous pouvez activer une connexion LDAP existante afin d'établir une connexion entre le Control Panel et un service d'annuaire. Après l'activation de la connexion LDAP, il est à nouveau possible de synchroniser les utilisateurs et leurs appartenances à des groupes depuis le service d'annuaire dans le Control Panel (voir Ajouter une connexion LDAP à la page 125) et d'utiliser les identifiants du service d'annuaire

pour la connexion au Control Panel (voir Configurer une connexion dans le Control Panel via LDAP à la page 135).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez activer la connexion LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Actionnez le bouton **Activer connexion LDAP**.

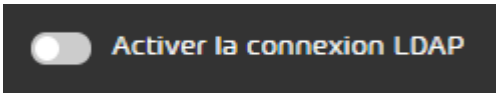


Illustration 110 : Désactiver la connexion LDAP

Le bouton devient vert. Le bouton **Tester la synchronisation LDAP** sous **Synchronisation d'utilisateurs et de groupes** est déverrouillé.

6. Cliquez sur **Appliquer les modifications**.

Les paramètres sont mémorisés.

> **REMARQUE :**
>
> La synchronisation des données à partir du service d'annuaire a lieu dans une cadence horaire. Il se peut donc que le résultat des paramètres n'apparaîsse pas avant deux heures.

Une connexion LDAP existante a été activée.

Supprimer une connexion LDAP

Vous avez ajouté une connexion LDAP au Control Panel (voir Ajouter une connexion LDAP à la page 125).

L'onglet **Connexion LDAP** (voir Connexion LDAP à la page 122) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet de supprimer une connexion LDAP existante si elle n'est plus nécessaire. Après la suppression, les utilisateurs dont les boîtes aux lettres ont été préalablement synchronisées avec le service d'annuaire restent dans le Control Panel en tant que boîtes aux lettres LDAP. Cependant, les boîtes aux lettres ne sont plus synchronisées. Si les utilisateurs ont préalablement utilisé leurs identifiants du service d'annuaire pour se connecter au Control Panel, le dernier mot de passe synchronisé reste enregistré dans le Control Panel et les utilisateurs peuvent modifier leur mot de passe dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez supprimer la connexion LDAP.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Connexion LDAP**.
5. Sous **Connexions LDAP disponibles**, sélectionnez la connexion LDAP que vous souhaitez supprimer et cliquez sur la flèche de menu à côté de la connexion LDAP.

Illustration 111 : Ouvrir le menu

- Un menu s'ouvre.

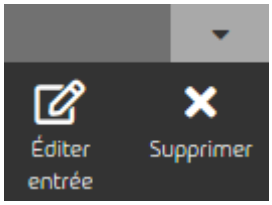


Illustration 112 : Menu

6. Cliquez sur **Supprimer**.

- Un message d'avertissement apparaît.

7. Cliquez sur **Confirmer**.

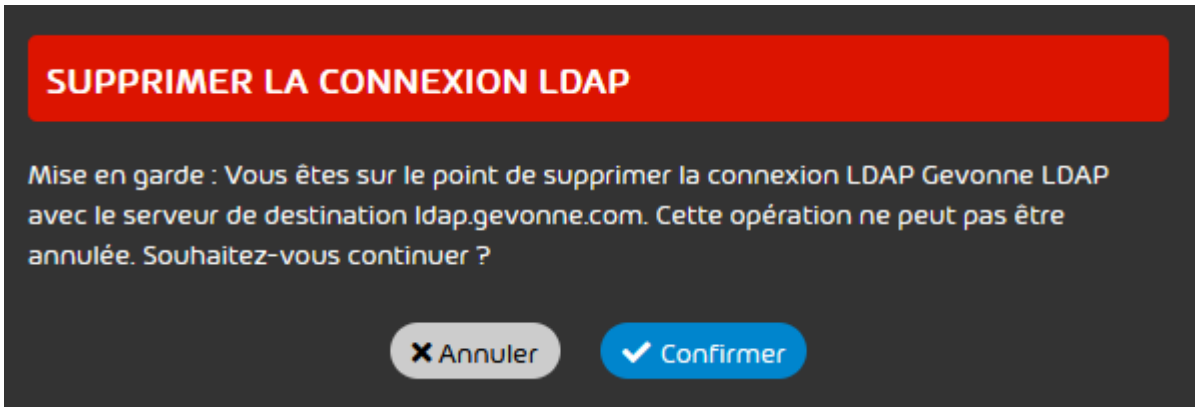


Illustration 113 : Confirmer la suppression

La connexion LDAP est supprimée de la liste sous **Connexions LDAP disponibles**.

Une connexion LDAP a été supprimée du Control Panel.

Régler les valeurs par défaut pour le fuseau horaire et la langue

Le module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet de définir des valeurs par défaut pour le fuseau horaire, la langue, le format de la date et de l'heure pour un client. Les paramètres s'appliquent à l'affichage dans le Control Panel et aux courriels automatiques du Control Panel.

REMARQUE :

Les valeurs par défaut sont transmises par tous les utilisateurs subordonnés. Dès qu'un utilisateur du client règle ses propres paramètres, les valeurs par défaut pour cet utilisateur seront écrasées. Les utilisateurs peuvent modifier les paramètres dans leurs paramètres utilisateur (voir le chapitre « Modifier le fuseau horaire et la langue » dans le manuel du Control Panel).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le client pour lequel vous souhaitez définir des valeurs par défaut.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Fuseau horaire et langue par défaut**.

Les paramètres du fuseau horaire, de la langue, du format de la date et de l'heure sont affichés dans la section **Fuseau horaire et langue**.

Illustration 114 : Fuseau horaire et langue

5. Dans le menu déroulant **Fuseau horaire**, sélectionnez un fuseau horaire.

> **REMARQUE :**
>
> Le fuseau horaire détermine le format des chiffres dans le Control Panel et dans les courriels automatiques du Control Panel.

6. Dans le menu déroulant **Langue**, sélectionnez une langue.

7. Dans le menu déroulant **Format de date**, sélectionnez un format de date.

> **REMARQUE :**
>
> Le format de date détermine l'ordre dans lequel les données disponibles d'une date sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

8. Dans le menu déroulant **Format d'heure**, sélectionnez un format d'heure.

> **REMARQUE :**
>
> Le format d'heure détermine l'ordre dans lequel les données disponibles d'une heure sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

9. Cliquez sur **Enregistrer**.

Les modifications sont enregistrées.

Des valeurs par défaut ont été définies pour le fuseau horaire, la langue, le format de la date et de l'heure pour un client.

Conditions générales

L'onglet **Termes et conditions** du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) permet aux administrateurs côté partenaires de définir un contrat de licence d'utilisateur final et un contrat de traitement des données afin d'obtenir l'accord des utilisateurs de leurs clients concernant les conditions contractuelles.

Une fois le contrat de licence d'utilisateur final et le contrat de traitement des données d'un partenaire publiés, les contrats sont présentés aux utilisateurs des clients lors de leur prochaine connexion au Control Panel. Pour pouvoir accéder au Control Panel, les utilisateurs doivent accepter le contrat de licence d'utilisateur final. Les administrateurs peuvent également accepter le contrat de traitement des données. Le consentement au contrat de traitement des données est facultatif

par défaut. Toutefois, les administrateurs côté partenaires peuvent également rendre obligatoire le consentement au contrat de traitement des données.

Pour pouvoir définir des termes et conditions, les administrateurs côté partenaires doivent d'abord activer les termes et conditions (voir Activer les conditions générales à la page 148). Cela permet d'activer les paramètres concernant les termes et conditions du partenaire. Les administrateurs peuvent ensuite rendre obligatoire le consentement au contrat de traitement des données pour les administrateurs de leurs clients (voir Rendre le contrat de traitement des données obligatoire à la page 149) et créer et publier un contrat de licence d'utilisateur final et un contrat de traitement des données (voir Rédiger un contrat de licence d' utilisateur final et un contrat de traitement des données à la page 151). Les contrats peuvent être rédigés dans toutes les langues du Control Panel. Si les conditions contractuelles d'un partenaire changent, les administrateurs du partenaire peuvent publier une nouvelle version des contrats.

REMARQUE :

Les versions précédentes des contrats ne sont pas enregistrées dans le Control Panel. L'onglet **Termes et conditions** du module **Tableau de bord des services** n'affiche que la version actuelle des contrats.

Les administrateurs côté partenaires peuvent exporter le texte de la version actuelle du contrat de licence d'utilisateur final et du contrat de traitement des données depuis le Control Panel (voir Exporter le contrat de licence d' utilisateur final et le contrat de traitement des données à la page 157) afin d'également pouvoir accéder à ces contrats à l'avenir. Si un partenaire ne souhaite plus utiliser les termes et conditions dans le Control Panel, les administrateurs du partenaire peuvent désactiver les termes et conditions (voir Désactiver les conditions générales à la page 158).

Les modifications apportées aux termes et conditions sont audités dans le module **Rapports & conformité** > **Audit 2.0** (voir le chapitre « Auditing 2.0 » dans le manuel du Control Panel).

Activer les conditions générales

Si vous souhaitez obtenir le consentement des utilisateurs de vos clients pour un contrat de licence d'utilisateur final et un contrat de traitement de données dans le Control Panel, vous devez d'abord activer les conditions générales pour un partenaire dans l'onglet **Termes et conditions** (voir

Conditions générales à la page 147) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le partenaire pour lequel vous souhaitez activer les conditions générales.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Termes et conditions**.
5. Actionnez le bouton **Activer les termes et conditions**.

Illustration 115 : Activer les conditions générales

Le bouton devient vert. Les autres paramètres de l'onglet **Termes et conditions** sont activés.

> **REMARQUE :**
>
> Si des paramètres sont déjà enregistrés dans l'onglet **Termes et conditions**, les paramètres seront à nouveau appliqués.

Les conditions générales ont été activées pour un partenaire.

Vous pouvez ensuite rendre le consentement au contrat de traitement des données obligatoire pour les administrateurs de vos clients (voir Rendre le contrat de traitement des données obligatoire à la page 149) ainsi que rédiger et publier un contrat de licence d'utilisateur final et un contrat de traitement de données (voir Rédiger un contrat de licence d' utilisateur final et un contrat de traitement des données à la page 151).

Rendre le contrat de traitement des données obligatoire

Vous avez activé les conditions générales (voir Activer les conditions générales à la page 148).

Si, dans l'onglet **Termes et conditions** (voir Conditions générales à la page 147) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous publiez un contrat de licence d'utilisateur final et un contrat de traitement des données, les utilisateurs de vos clients devront accepter le contrat de licence d'utilisateur final lors de leur prochaine connexion au Control Panel afin de pouvoir accéder à ce dernier. Les administrateurs de vos clients peuvent également accepter le contrat de traitement des données. Le consentement au contrat de traitement des données est facultatif par défaut. Cependant, vous avez également la possibilité de rendre obligatoire le consentement des administrateurs de vos clients au contrat de traitement des données.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le partenaire pour lequel vous souhaitez activer les conditions générales.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Termes et conditions**.
5. Actionnez le bouton **Rendre le contrat de traitement de données obligatoire**.

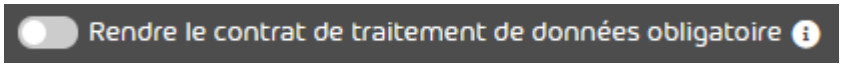


Illustration 116 : Rendre obligatoire le consentement au contrat de traitement des données

Le bouton devient vert. Si un contrat de licence d'utilisateur final et un contrat de traitement des données sont publiés pour le partenaire, les administrateurs des clients subordonnés du partenaire devront accepter le contrat de traitement des données en plus du contrat de licence d'utilisateur final afin d'accéder au Control Panel.

Le consentement au contrat de traitement des données a été rendu obligatoire.

Vous pouvez ensuite créer et publier un contrat de licence pour utilisateur final et un contrat de traitement des données (voir Rédiger un contrat de licence d' utilisateur final et un contrat de traitement des données à la page 151).

Rédiger un contrat de licence d’ utilisateur final et un contrat de traitement des données

L'onglet **Termes et conditions** (voir Conditions générales à la page 147) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet de créer et de publier un contrat de licence d'utilisateur final et un contrat de traitement des données Les contrats seront présentés aux utilisateurs de vos clients lors de leur prochaine connexion au Control Panel. Pour accéder au Control Panel, les utilisateurs doivent accepter le contrat de licence d'utilisateur final. Les administrateurs de vos clients peuvent également accepter le contrat de traitement des données. En cas de modifications des conditions contractuelles, vous pouvez créer et publier une nouvelle version des contrats. Dès qu'une nouvelle version est publiée, les utilisateurs devront à nouveau accepter les conditions contractuelles.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le partenaire pour lequel vous souhaitez activer les conditions générales.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Termes et conditions**.
5. Dans **Contenu du contrat de licence d'utilisateur final et du contrat de traitement de données**, cliquez sur **Créer une nouvelle version**.

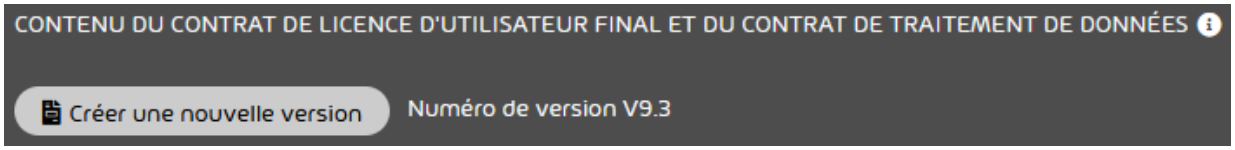


Illustration 117 : Créer une nouvelle version

> **REMARQUE :**
>
> Si une version existe déjà, le numéro de version précédent apparaît à droite du bouton **Créer une nouvelle version**.

Une fenêtre de confirmation apparaît.

6. Cliquez sur **Créer une nouvelle version**.

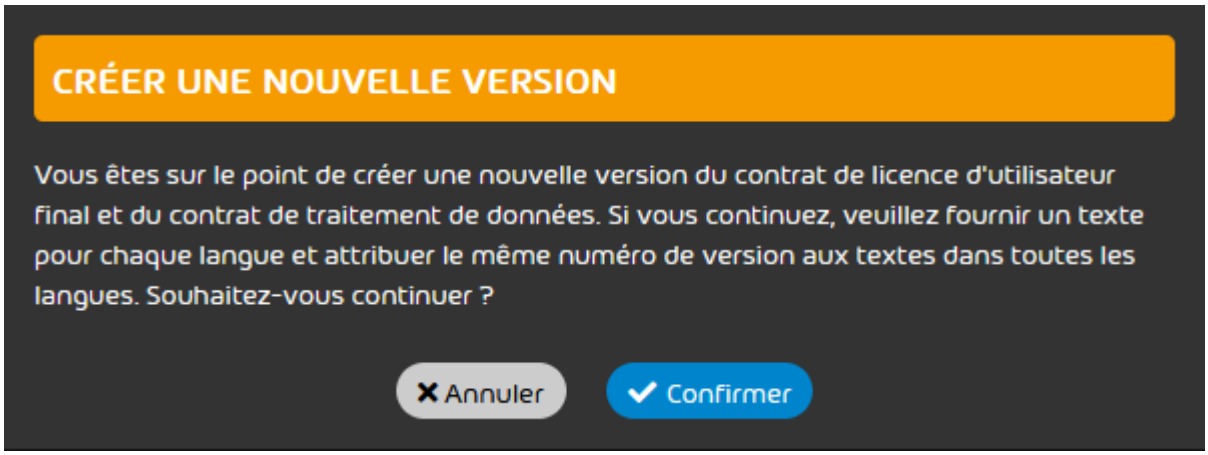


Illustration 118 : Confirmer la création d' une nouvelle version

- Un champ de saisie pour le nouveau numéro de version apparaît à côté de l'ancien numéro de version.

Illustration 119 : Champ de saisie pour le nouveau numéro de version

7. Saisissez le nouveau numéro de version dans le champ de saisie.

> **REMARQUE :**
>
> Les numéros de version qui sont attribués aux versions précédentes ne sont pas acceptés.
>
> Le numéro de version peut contenir les caractères suivants :
>
> - Points
> - Lettres
> - Chiffres
>
> Les points ne sont pas autorisés au début ni à la fin. Deux points consécutifs ou plus ne sont pas autorisés.

8. Dans le menu déroulant **Langue**, sélectionnez la langue pour laquelle vous souhaitez créer un texte.

Illustration 120 : Sélectionner la langue

> **REMARQUE :**
>
> Le texte du contrat de licence d'utilisateur final et du contrat de traitement des données peut être rédigé dans n'importe quelle langue du Control Panel. Les contrats sont présentés à tous les utilisateurs des clients subordonnés, peu importe que le texte soit rédigé dans la langue d'affichage des utilisateurs ou non.

L'éditeur de texte apparaît vide.

Illustration 121 : Éditeur de texte

REMARQUE :

Les langues d'affichage du Control Panel sont affichées dans la partie inférieure de l'éditeur de texte. Les langues pour lesquelles un texte a déjà été publié dans cette version apparaissent sur fond blanc. Les langues non utilisées sont grisées.

9. Facultatif : Si vous souhaitez copier le texte de la version précédente dans l'éditeur de texte, cliquez sur **Restaurer le contenu de la version antérieure**.

➔ Si un texte a été publié dans la langue sélectionnée pour la version précédente, ce texte apparaîtra dans l'éditeur de texte.

10. Facultatif : Si vous souhaitez importer un texte à partir de votre système de fichiers dans l'éditeur de texte, suivez les étapes suivantes.

a) Cliquez sur **Importer un texte**.

➔ Un affichage étendu s'ouvre.

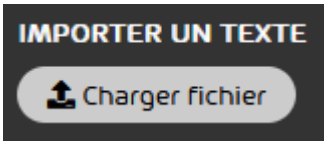


Illustration 122 : Vue élargie

b) Cliquez sur **Charger fichier**.

➔ Une fenêtre de sélection des fichiers s'ouvre.

c) Sélectionnez le fichier dont vous souhaitez importer le contenu.

> **REMARQUE :**
>
> Seuls les fichiers .txt peuvent être importés.

➔ Le Control Panel lit le fichier et prépare le contenu du fichier pour l'importation.

d) Cliquez sur **Importer**.

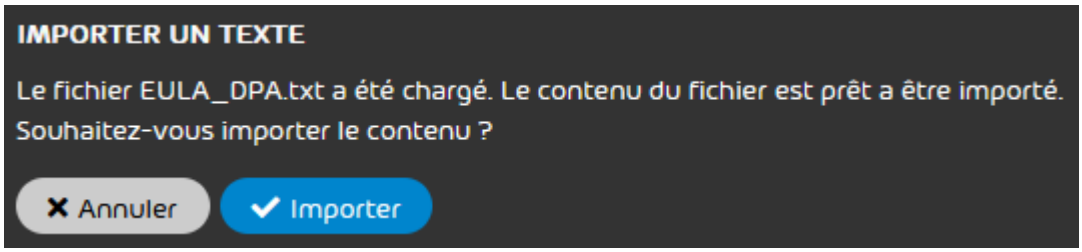


Illustration 123 : Confirmer l' importation

➔ Le texte provenant du fichier importé apparaît dans l'éditeur de texte.

11. Facultatif : Saisissez le texte du contrat de licence d'utilisateur final et du contrat de traitement des données dans l'éditeur de texte ou éditez le texte existant selon vos souhaits.

> **REMARQUE :**
>
> Il n'est pas possible de formater le texte.

12. Dès que le texte est prêt pour la publication, cliquez sur **Publier** dans l'éditeur de texte.

Illustration 124 : Publier le texte

- Une fenêtre de confirmation apparaît.

13. Cliquez sur **Confirmer**.

Illustration 125 : Confirmer la publication

- Le texte dans la langue sélectionnée est publié. La nouvelle version du contrat de licence d'utilisateur final et du contrat de traitement des données sera présentée à tous les utilisateurs des clients subordonnés lors de leur prochaine connexion au Control Panel. Les utilisateurs doivent accepter le contrat de licence d'utilisateur final afin de pouvoir accéder au Control Panel. Les administrateurs des clients subordonnés peuvent également accepter le contrat de traitement des données.

14. Répétez les étapes 8 à la page 153 à 13 à la page 156 pour toutes les langues dans lesquelles vous souhaitez ajouter un texte du contrat de licence d'utilisateur final et du contrat de traitement des données.

Une nouvelle version du contrat de licence d'utilisateur final et du contrat de traitement des données a été créée et publiée.

Vous pouvez ensuite exporter le contrat de licence d'utilisateur final et le contrat de traitement des données dans leur version actuelle (voir Exporter le contrat de licence d' utilisateur final et le contrat de traitement des données à la page 157).

Exporter le contrat de licence d' utilisateur final et le contrat de traitement des données

Vous avez créé et publié un contrat de licence de l'utilisateur final et un contrat de traitement des données (voir Rédiger un contrat de licence d' utilisateur final et un contrat de traitement des données à la page 151).

Dans l'onglet **Termes et conditions** (voir Conditions générales à la page 147) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100), vous pouvez exporter la version actuelle du contrat de licence de l'utilisateur final et du contrat de traitement des données. Cela permet d'enregistrer les contrats en dehors du Control Panel afin de pouvoir y accéder à nouveau ultérieurement.

REMARQUE :

Les versions précédentes des contrats ne sont pas enregistrées dans le Control Panel. L'onglet **Termes et conditions** du module **Tableau de bord des services** n'affiche que la version actuelle des contrats.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le partenaire pour lequel vous souhaitez activer les conditions générales.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Termes et conditions**.

5. Dans le menu déroulant **Langue**, sélectionnez la langue pour laquelle vous souhaitez exporter le texte.

Illustration 126 : Sélectionner la langue

- Dans l'éditeur de texte, le texte du contrat de licence de l'utilisateur final et du contrat de traitement des données apparaît dans la langue sélectionnée.

6. Au-dessus de l'éditeur de texte, cliquez sur **Exporter le texte**.

Illustration 127 : Exporter le texte

- Le texte du contrat de licence de l'utilisateur final et du contrat de traitement des données est exporté dans la langue sélectionnée sous forme de fichier .txt et disponible au téléchargement.

7. Enregistrez le fichier exporté sur votre système de fichier.
8. Répétez les étapes 5 à la page 158 à 7 à la page 158 pour toutes les langues dont vous souhaitez exporter les textes.

Le texte de la version actuelle du contrat de licence de l'utilisateur final et du contrat de traitement des données a été exporté.

Désactiver les conditions générales

Vous avez activé les conditions générales (voir Activer les conditions générales à la page 148).

L'onglet **Termes et conditions** (voir Conditions générales à la page 147) du module **Tableau de bord des services** (voir À propos du tableau de bord des services à la page 100) vous permet de désactiver les conditions générales. Une fois que vous avez désactivé les conditions générales, les

autres paramètres de l'onglet **Termes et conditions** sont bloqués. Les utilisateurs de vos clients ne verront plus de contrat de licence d'utilisateur final ni de contrat de traitement des données lorsqu'ils se connecteront au Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le partenaire pour lequel vous souhaitez activer les conditions générales.
3. Naviguez vers **Tableau de bord des services**.
4. Sélectionnez l'onglet **Termes et conditions**.
5. Actionnez le bouton **Activer les termes et conditions**.

Illustration 128 : Désactiver les conditions générales

Le bouton devient gris. Les autres paramètres de l'onglet **Termes et conditions** sont bloqués. Les utilisateurs des clients subordonnés ne verront plus de contrat de licence d'utilisateur final ni de contrat de traitement des données lorsqu'ils se connecteront au Control Panel.

> **REMARQUE :**
>
> Les paramètres précédents de l'onglet **Termes et conditions** sont conservés au cas où les conditions générales seraient réactivées par la suite (voir Activer les conditions générales à la page 148).

Les conditions générales ont été désactivées.

Vous pouvez ensuite réactiver les conditions générales (voir Activer les conditions générales à la page 148).

Rapports & conformité

Rapports & conformité

Le module **Rapports & conformité** regroupe des informations sur le trafic de courriels, les attaques sur les utilisateurs d'un domaine et les actions effectuées dans le Control Panel.

Dans le module subordonné **Statistiques des courriels**, les utilisateurs peuvent consulter les statistiques de leur propre trafic de courriels (voir Statistiques des courriels à la page 160). Les administrateurs côté clients et les utilisateurs avec le rôle **Service Desk** ou **Reporting** (voir Rôles à la page 49) peuvent également consulter dans ce module les statistiques sur le trafic de courriels de leur domaine ou d'un utilisateur de leur domaine.

Le module subordonné **Threat Live Report** est disponible pour les administrateurs côté clients et les utilisateurs avec le rôle **Service Desk** ou **Reporting** dans la mesure où Advanced Threat Protection est activée pour le client. Le module contient des informations concernant les attaques contre les utilisateurs du domaine (voir À propos du Threat Live Report à la page 174).

Le module subordonné **Audit 2.0** est disponible pour les administrateurs côté clients et côté partenaires. Dans le module, les actions effectuées par les utilisateurs dans le Control Panel sont auditées (voir Auditing 2.0 à la page 188).

Statistiques des courriels

Dans le module **Statistiques des courriels**, les utilisateurs peuvent consulter des statistiques sur leur propre trafic de courriels. En outre, les administrateurs côté clients peuvent consulter les statistiques sur le trafic de courriels de leur domaine ou d'un utilisateur de leur domaine.

Les utilisateurs peuvent choisir la période et le sens des courriels auxquelles les statistiques du module doivent se rapporter (voir Filtrer les statistiques de courriels à la page 161). Les statistiques sont présentées dans deux diagrammes. Le premier diagramme montre la répartition des courriels dans les catégories de courriels du Control Panel (voir Courriels par type à la page 163). Le deuxième diagramme montre la répartition temporelle des courriels (voir Courriels par

période à la page 164). Les données du deuxième diagramme peuvent également être exportées en tant que fichier CSV (voir Exporter les statistiques de courriels sous un fichier CSV à la page 166). En outre, les administrateurs côté clients peuvent voir comment les courriels des utilisateurs d'un domaine sont répartis entre les catégories de courriels dans le Control Panel (voir Courriels par utilisateur à la page 167).

En outre, les statistiques des courriels d'un domaine peuvent être résumées dans un rapport chaque mois (voir Rapport mensuel à la page 168). Les administrateurs côté clients peuvent définir à quelles boîtes aux lettres le rapport mensuel doit être envoyé (voir Ajouter des destinataires à la page 168). Au lieu d'ajouter des destinataires individuels, les administrateurs également importer une liste de destinataires à partir d'un fichier CSV (voir Importer des destinataires à partir d' un fichier CSV à la page 171). En outre, les administrateurs peuvent supprimer les destinataires existantes (voir Supprimer un destinataire à la page 173).

Filtrer les statistiques de courriels

Des statistiques concernant votre trafic de courriels sont affichées dans le module **Statistiques des courriels** (voir Courriels par type à la page 163 et Courriels par période à la page 164). En tant qu'administrateur côté client ou qu'utilisateur avec le rôle **Service Desk** ou **Reporting** , vous pouvez consulter les données du domaine d'un client au lieu de vos propres données. En outre, il est possible de voir pour un domaine comment les courriels des utilisateurs du domaine sont répartis entre les catégories de courriels dans le Control Panel (voir Courriels par utilisateur à la page 167). Dans le module **Statistiques des courriels**, vous pouvez filtrer les données selon une période et un sens de courriel.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Facultatif : Si vous souhaitez afficher les données d'un domaine ou d'un utilisateur d'un domaine au lieu de vos propres données, sélectionnez le domaine ou l'utilisateur dans la sélection de l'espace.
3. Naviguez vers **Rapports & conformité** > **Statistiques des courriels**.

4. Cliquez sur la période.

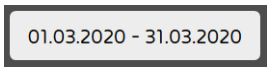


Illustration 129 : Cliquer sur la période

- Un calendrier apparaît.

5.

> **IMPORTANT :**
>
> Il est possible d'afficher au maximum les données des 3 derniers mois.

Sélectionnez une période.

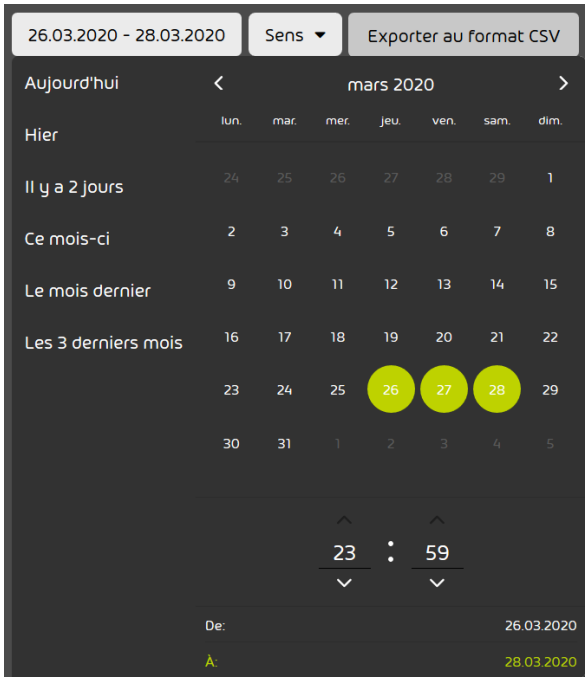


Illustration 130 : Sélectionner une période

- Dans le module **Statistiques des courriels**, seules les données des courriels de la périodes sélectionnée sont affichées.

6. Facultatif : Dans le menu déroulant **Sens**, sélectionnez le sens des courriels qui doivent être pris en compte dans les statistiques. Vous pouvez choisir parmi les options suivantes :

   - **Les deux** : les courriels entrants et sortants sont pris en compte dans les statistiques.
   - **Entrant** : seuls les courriels entrants sont pris en compte dans les statistiques.
   - **Sortant** : seuls les courriels sortants sont pris en compte dans les statistiques.

Illustration 131 : Sélectionner le sens

Dans le module **Statistiques des courriels**, seules les données des courriels du sens sélectionné sont affichées.

Les données du module **Statistiques des courriels** ont été filtrés en fonction d'une période et d'un sens de courriel.

Courriels par type

Le diagramme **Courriels par type** du module **Rapports & conformité** > **Statistiques des courriels** montre comment les courriels d'un utilisateur ou d'un domaine se répartissent dans les catégories de courriels du Control Panel (voir Catégories de courriels à la page 84).

REMARQUE :

Les utilisateurs simples peuvent consulter les données du diagramme concernant leur propre trafic de courriels. Les administrateurs côté clients et les utilisateurs avec le rôle **Service Desk** ou **Reporting** (voir Rôles à la page 49) peuvent également consulter les données d'un domaine ou d'un utilisateur d'un domaine au lieu de leurs propres données. Les données affichées peuvent être filtrées en fonction d'une période et d'un sens de courriel (voir Filtrer les statistiques de courriels à la page 161).

Le diagramme indique le nombre total de courriels reçus et/ou envoyés dans la période sélectionnée. En outre, le diagramme indique le nombre et le pourcentage de courriels attribués à chaque catégorie de courriels dans le Control Panel.

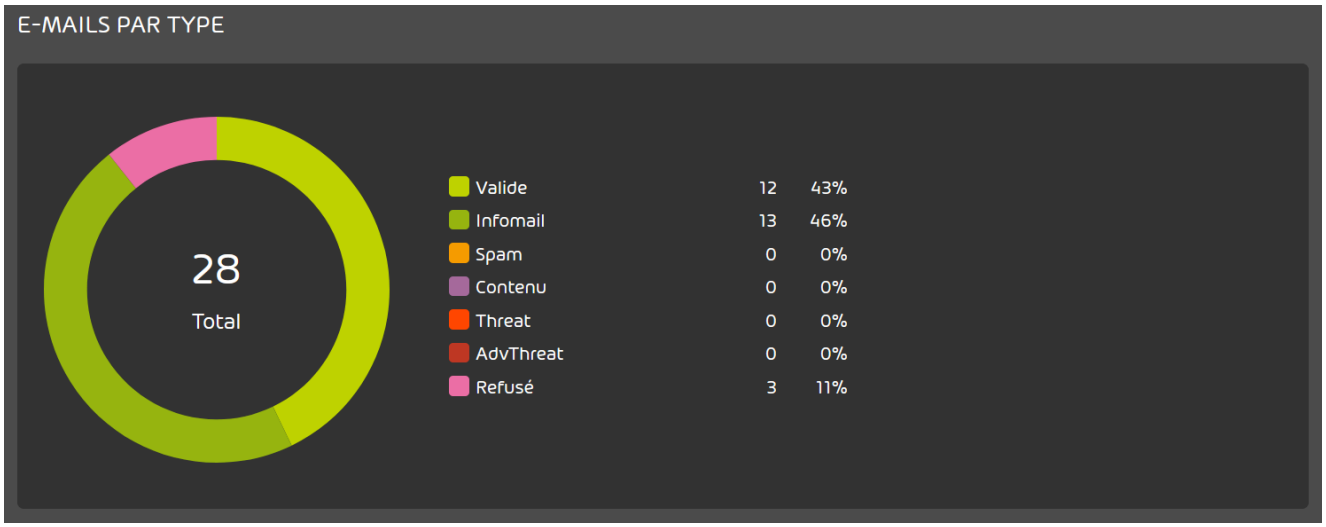


Illustration 132 : Courriels par type

Courriels par période

La statistique **Courriels par période** montre une vue d'ensemble des courriels entrants et/ou sortants dans la période sélectionnée. Dans la statistique, le nombre de courriels est présenté par catégorie en chiffres absolus.

REMARQUE :

Les utilisateurs simples peuvent consulter les données du diagramme concernant leur propre trafic de courriels. Les administrateurs côté clients et les utilisateurs avec le rôle **Service Desk** ou **Reporting** (voir Rôles à la page 49) peuvent également consulter les données d'un domaine ou d'un utilisateur d'un domaine au lieu de leurs propres données. Les données affichées peuvent être filtrées en fonction d'une période et d'un sens de courriel (voir Filtrer les statistiques de courriels à la page 161).

Le diagramme montre le nombre de courriels qui ont été reçus et/ou envoyés à différents moments pendant la période sélectionnée. Le diagramme est réparti par couleurs selon les catégories de courriels (voir Catégories de courriels à la page 84).

Dès que le curseur passe sur un point du diagramme, un aperçu du nombre de courriels de chaque catégorie reçus et/ou envoyés à ce moment s'affiche dès que possible. À ce moment apparaît également une ligne verticale sur laquelle se trouvent des points correspondant aux différentes catégories de courriels. Dès que le curseur passe sur l'un de ces points, le nombre de courriels de cette catégorie apparaît.

En outre, les données du diagramme peuvent être exportées sous forme de fichier CSV (voir Exporter les statistiques de courriels sous un fichier CSV à la page 166).

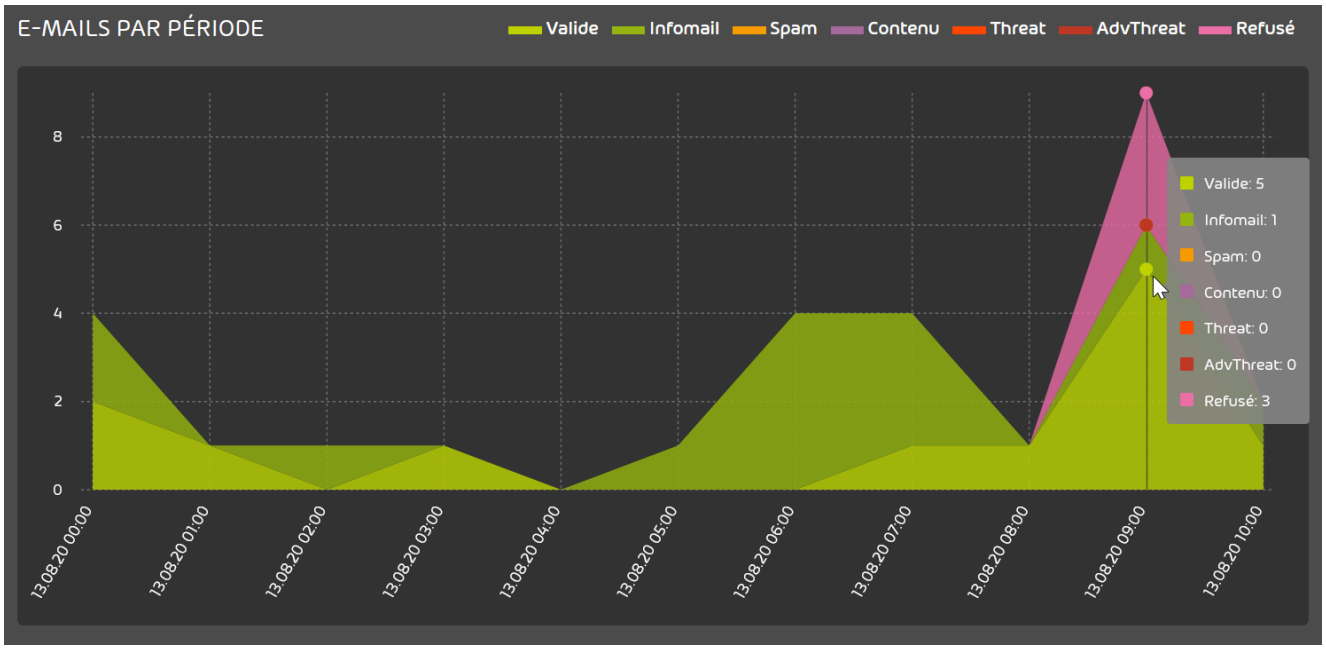


Illustration 133 : Courriels par période

Exporter les statistiques de courriels sous un fichier CSV

Dans le module **Statistiques des courriels**, il y a un diagramme qui montre la répartition temporelle des courriels (voir Courriels par période à la page 164). Vous pouvez exporter les données de ce diagramme en tant que fichier CSV. En tant qu'administrateur côté client ou qu'utilisateur avec le rôle **Service Desk** ou **Reporting** (voir Rôles à la page 49), vous pouvez exporter soit vos propres données, soit les données de votre domaine ou d'un utilisateur de votre domaine.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Facultatif : Si vous souhaitez exporter les données d'un domaine ou d'un utilisateur d'un domaine au lieu de vos propres données, sélectionnez le domaine ou l'utilisateur dans la sélection de l'espace.
3. Naviguez vers **Rapports & conformité** > **Statistiques des courriels**.

4. Sélectionnez une période et un sens de courriels pour les statistiques (voir Filtrer les statistiques de courriels à la page 161).

Seuls les courriels de la période et du sens sélectionnés sont pris en compte dans les statistiques.

5. Cliquez sur **Exporter au format CSV**.

Illustration 134 : Exporter en tant que fichier CSV

Un fichier CSV contenant les données du diagramme de la répartition temporelle des courriels est disponible au téléchargement.

6. Téléchargez le fichier.

Les données du diagramme de la répartition temporelle des courriels ont été téléchargées.

Courriels par utilisateur

Les statistiques **Courriels par utilisateur pour les 7 derniers jours (top 100)** dans le module **Rapports & conformité** > **Statistiques des courriels** sont disponibles pour les administrateurs côté clients ainsi que pour les utilisateurs avec le rôle **Service Desk** ou **Reporting** (voir Rôles à la page 49). Les statistiques ne sont affichées que si un domaine a été sélectionné dans la sélection de l'espace (voir Filtrer les statistiques de courriels à la page 161). Les statistiques peuvent être filtrées selon le sens du courriel (voir Filtrer les statistiques de courriels à la page 161).

Les statistiques répertorient les 100 utilisateurs du domaine qui ont reçu et/ou envoyé le plus de courriels au cours des 7 derniers jours. Les utilisateurs sont classés en fonction du nombre total de leurs courriels. En outre, le nombre de courriels est affiché pour chaque catégorie de courriels (voir Catégories de courriels à la page 84).

E-MAILS PAR UTILISATEUR POUR LES 7 DERNIERS JOURS (TOP 100)

Boîte aux lettres	Valide	Infomail	Spam	Contenu	Threat	AdvThre...	Refusé	Total
[redacted]	306	70	3	156	26	8	4	573
[redacted]	66	123	6	0	0	0	16	211
[redacted]	178	0	0	0	0	0	0	178
[redacted]	2	87	0	0	0	2	1	92
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	16	31	2	0	0	0	1	50

Illustration 135 : Courriels par utilisateur

Rapport mensuel

Les statistiques des courriels d'un domaine peuvent être résumées dans un rapport chaque mois. Le rapport mensuel est envoyé aux destinataires sélectionnés au début de chaque mois et résume les statistiques des courriels du mois précédent.

Les administrateurs côté clients peuvent sélectionner les destinataires auxquels le rapport mensuel doit être envoyé. Le rapport mensuel peut être envoyé aux utilisateurs du domaine ainsi qu'à des boîtes aux lettres externes. Les administrateurs peuvent soit ajouter des destinataires individuellement (voir Ajouter des destinataires à la page 168), soit importer une liste de destinataires à partir d'un fichier CSV (voir Importer des destinataires à partir d' un fichier CSV à la page 171). Pour ces fichiers CSV, les exigences spécifiques s'appliquent (voir Fichiers CSV pour importer des destinataires à la page 172). Lorsqu'un destinataire n'est plus nécessaire, les administrateurs peuvent le supprimer (voir Supprimer un destinataire à la page 173).

Ajouter des destinataires

Une fois par mois, un rapport contenant les statistiques des courriels (voir Statistiques des courriels à la page 160) du mois précédent est envoyé aux destinataires sélectionnés pour chaque domaine. Vous pouvez ajouter individuellement les utilisateurs de votre domaine et les boîtes aux lettres externes comme destinataires.

REMARQUE :

Les utilisateurs du Control Panel reçoivent le rapport mensuel dans la langue réglée dans leurs paramètres utilisateur (voir le chapitre « Modifier le fuseau horaire et la langue » dans le manuel du Control Panel). Les destinataires externes reçoivent le rapport mensuel en anglais.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez définir des destinataires pour le rapport mensuel correspondant.
3. Naviguez vers **Rapports & conformité** > **Statistiques des courriels**.
4. Cliquez sur **Envoyer par courriel**.

Illustration 136 : Ouvrir les paramètres du rapport mensuel

Les paramètres du rapport mensuel sont affichés.

5. Facultatif : Si vous voulez spécifier un utilisateur du domaine comme destinataire, procédez comme suit.

   a) Dans le champ de recherche sous **Boîtes aux lettres**, tapez l'adresse courriel de l'utilisateur et cliquez sur Entrée.

Les résultats de recherche sont affichés dans la liste située sous le champ de recherche.

Illustration 137 : Résultats de recherche

b) Cliquez sur l'adresse courriel de l'utilisateur dans la liste.

L'adresse courriel est ajoutée à la liste des destinataires.

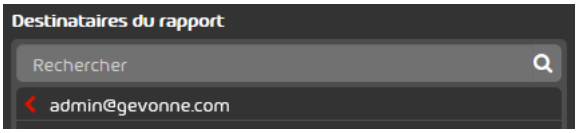


Illustration 138 : Liste des destinataires

6. Facultatif : Si vous souhaitez spécifier une boîte aux lettres externe comme destinataire, procédez comme suit.

a) Saisissez l'adresse courriel externe dans le champ **Boîte aux lettres externe**.

Le bouton **Ajouter** est déverrouillé.

b) Cliquez sur **Ajouter**.

Illustration 139 : Ajouter une boîte aux lettres externe

L'adresse courriel externe est ajoutée à la liste des destinataires.

7. Cliquez sur **Appliquer les modifications**.

Les modifications sont acceptées.

Des destinataires individuels ont été définis pour le rapport mensuel.

Importer des destinataires à partir d’ un fichier CSV

Une fois par mois, un rapport contenant les statistiques des courriels (voir Statistiques des courriels à la page 160) du mois précédent est envoyé aux destinataires sélectionnés pour chaque domaine. Vous pouvez importer de nouveaux destinataires à partir d'un fichier CSV. Le fichier CSV peut contenir des utilisateurs du domaine ainsi que des boîtes aux lettres externes.

REMARQUE :

Les utilisateurs du Control Panel reçoivent le rapport mensuel dans la langue réglée dans leurs paramètres utilisateur (voir le chapitre « Modifier le fuseau horaire et la langue » dans le manuel du Control Panel). Les destinataires externes reçoivent le rapport mensuel en anglais.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez définir des destinataires pour le rapport mensuel correspondant.
3. Naviguez vers **Rapports & conformité** > **Statistiques des courriels**.
4. Cliquez sur **Envoyer par courriel**.

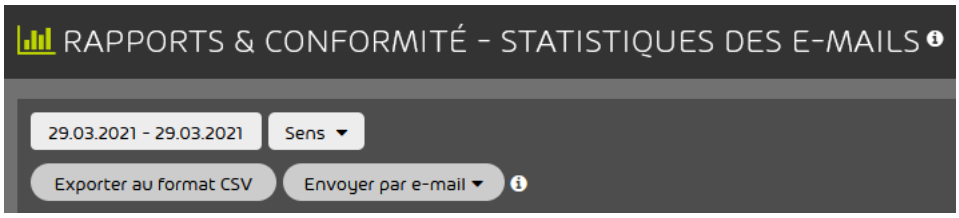


Illustration 140 : Ouvrir les paramètres du rapport mensuel

Les paramètres du rapport mensuel sont affichés.

5. Cliquez sur **Importer liste à partir d'un fichier CSV**.

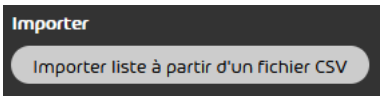


Illustration 141 : Importer une liste à partir d' un fichier CSV

- Une fenêtre de sélection des fichiers s'ouvre.

6. **IMPORTANT :**

   Pour s'assurer qu'un fichier CSV externe peut être importé dans le Control Panel sans erreur, des règles doivent être observées concernant le format du fichier, sa structure de contenu et une syntaxe valide (voir Fichiers CSV pour importer des destinataires à la page 172).

   Sélectionnez le fichier CSV désiré.

- Les adresses courriel du fichier CSV sont ajoutées à la liste des destinataires.

Pour le rapport mensuel, les destinataires ont été importés à partir d'un fichier CSV.

Fichiers CSV pour importer des destinataires

Pour le rapport mensuel, une liste de destinataires peut être importée à partir d'un fichier CSV (voir Importer des destinataires à partir d' un fichier CSV à la page 171). Pour garantir qu'un fichier CSV externe contenant les destinataires du rapport mensuel puisse être importé dans le Control Panel sans erreur, des règles doivent être observées pour l'extension des fichiers et la structure du contenu. Le fichier CSV peut contenir les adresses courriel des utilisateurs du panneau de contrôle ainsi que les adresses courriel des boîtes aux lettres externes.

Règles pour l' extension des fichiers

- L'extension du fichier à importer est **.csv**. Les autres extensions de fichier telles que .txt ou .docx ne seront pas acceptées.

Règles pour les colonnes et les lignes

- Le fichier CSV ne contient qu'une seule colonne.
- La première ligne contient le nom de la colonne. Le nom de la colonne peut être choisi librement.
- Le fichier CSV contient une adresse courriel de chaque destinataire à partir de la deuxième ligne.
- Les lignes ne se terminent pas par un signe de ponctuation.

Règle de conformité des adresses courriel

- Les adresses courriel doivent être bien formées (selon le modèle « partielocale@nomhote.domaine-principal »).

> **IMPORTANT :**
>
> Les adresses mal formées ne sont pas prises en compte lors de l'importation.

Règle pour les doublons

- Les doublons n'ont aucune influence sur le traitement du fichier CSV, mais doivent être évités.

Supprimer un destinataire

Vous avez défini les destinataires du rapport mensuel (voir Ajouter des destinataires à la page 168 ou Importer des destinataires à partir d'un fichier CSV à la page 171).

Si vous ne souhaitez pas qu'un destinataire reçoive le rapport mensuel à l'avenir, vous pouvez le supprimer.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez définir des destinataires pour le rapport mensuel correspondant.
3. Naviguez vers **Rapports & conformité** > **Statistiques des courriels**.

4. Cliquez sur **Envoyer par courriel**.

Illustration 142 : Ouvrir les paramètres du rapport mensuel

Les paramètres du rapport mensuel sont affichés.

5. Dans la liste des destinataires, cliquez sur le destinataire que vous souhaitez supprimer.

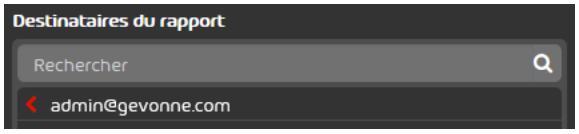


Illustration 143 : Supprimer le destinataire

Le destinataire est supprimé de la liste.

Un destinataire du rapport mensuel a été supprimé.

Threat Live Report

À propos du Threat Live Report

> **IMPORTANT :**
>
> Le Threat Live Report est uniquement disponible pour les clients qui ont commandé l'**Advanced Threat Protection**.

Vous trouverez également des informations sur les différents diagrammes directement dans l'interface. Pour cela, passez sur le derrière le nom de la statistique ou du diagramme.

Description des statistiques

Vue d’ ensemble des attaques en temps réel

Sous **Vue d'ensemble des attaques en temps réel** dans **Threat Live Report** vous trouverez en temps réel toutes les attaques interceptées pour votre entreprise ou pour tous les utilisateurs du Control Panel dans le monde (voir Basculer entre les données globales et les données spécifiques au domaine à la page 185). L'origine, la cible et le type de menace sont affichés dans un tableau. Vous trouverez une liste de tous les types de menaces dans Description des types d’ attaques à la page 180.

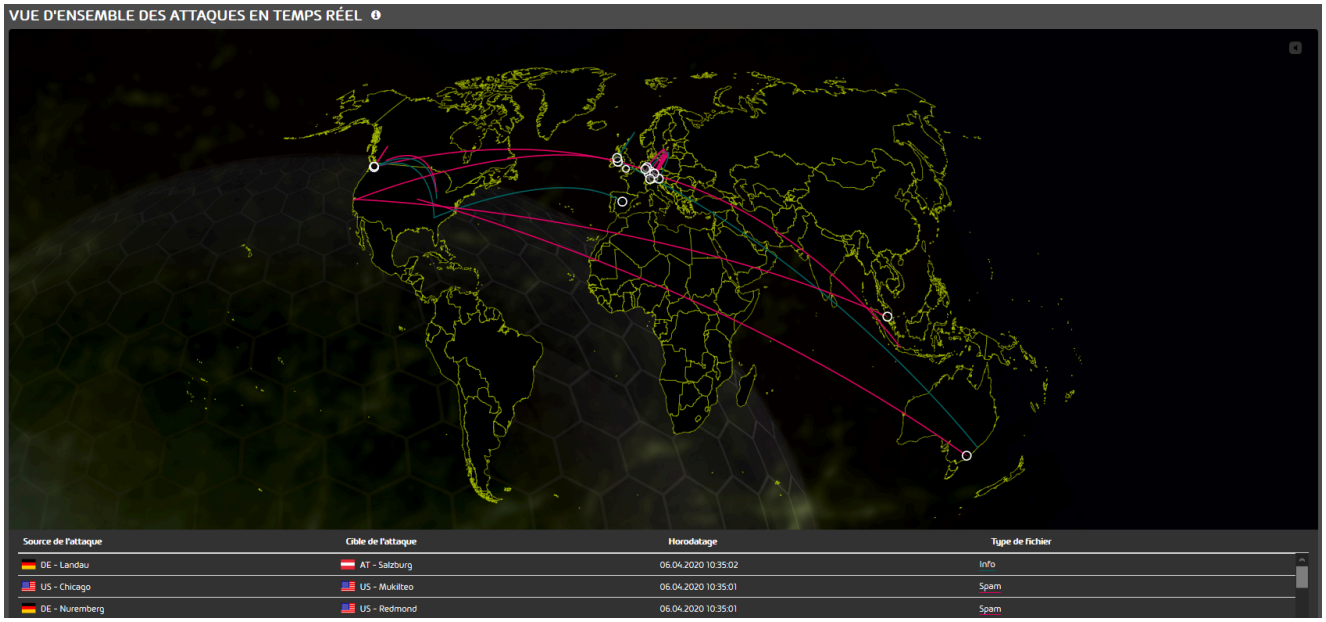


Illustration 144 : Vue d’ ensemble des attaques en temps réel

Attaques tentées - Type d’ attaque par date

La statistique **Type d'attaque par date** dans le **Threat Live Report** montre combien d'attaques ont eu lieu par type d'attaque à un moment précis dans la période sélectionnée. Les données peuvent se référer soit au domaine actuellement sélectionné, soit à tous les clients (voir Basculer entre les données globales et les données spécifiques au domaine à la page 185).

Pour visualiser le nombre absolu d'attaques par type d'attaque à un moment précis, vous pouvez déplacer la souris sur les lignes verticales. Si la souris se trouve sur l'un des points d'un type d'attaque, seuls le diagramme associé et les informations sur le nombre d'attaques sont affichés.

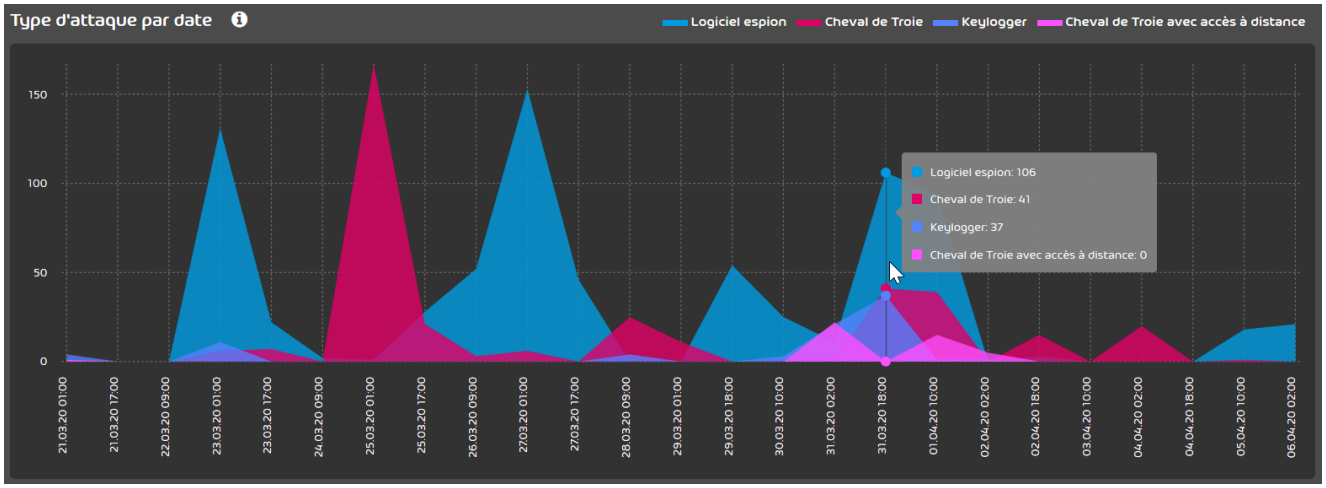


Illustration 145 : Attaques tentées - Type d' attaque par date

Statistiques des menaces - Par type d' attaque

Le diagramme **Par type d'attaque** dans **Threat Live Report** montre la distribution des attaques dans la période sélectionnée en fonction de leur type d'attaque. Le nombre total d'attaques survenues au cours de la période sélectionnée est affiché au centre. Les données peuvent se référer soit au domaine actuellement sélectionné, soit à tous les clients (voir Basculer entre les données globales et les données spécifiques au domaine à la page 185). Vous trouverez une description des types d'attaque sous Description des types d' attaques à la page 180.

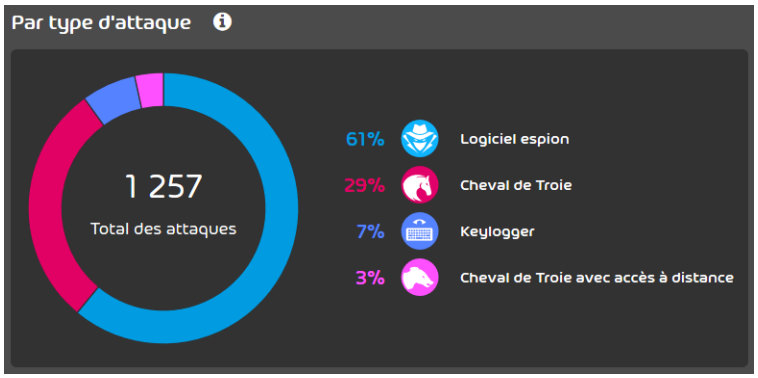


Illustration 146 : Statistiques des menaces - Par type d'attaque

Statistiques des menaces - Par vecteur d'attaque

Le diagramme **Par vecteur d'attaque** dans **Threat Live Report** montre la distribution des attaques dans la période sélectionnée en fonction de leur vecteur d'attaque. Le nombre total d'attaques survenues au cours de la période sélectionnée est affiché au centre. Les données peuvent se référer soit au domaine actuellement sélectionné, soit à tous les clients (voir Basculer entre les données globales et les données spécifiques au domaine à la page 185). Vous trouverez une description des vecteurs d'attaque sous Description des vecteurs d'attaques à la page 183.

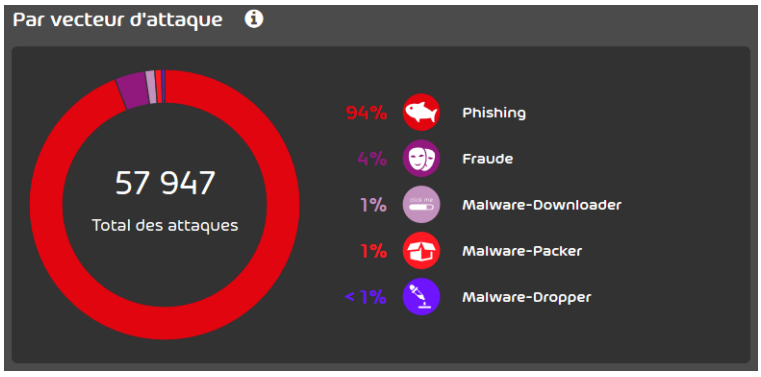


Illustration 147 : Statistiques des menaces - Par vecteur d'attaque

Attaques tentées - Vecteur d’ attaque par date

La statistique **Vecteurs d'attaque par date** dans le **Threat Live Report** montre combien d'attaques ont eu lieu par vecteur d'attaque à un moment précis dans la période sélectionnée. Les données peuvent se référer soit au domaine actuellement sélectionné, soit à tous les clients (voir Basculer entre les données globales et les données spécifiques au domaine à la page 185).

Pour visualiser le nombre absolu d'attaques par vecteur d'attaque à un moment précis, vous pouvez déplacer la souris sur les lignes verticales. Si la souris se trouve sur l'un des points d'un vecteur d'attaque, seuls le diagramme associé et les informations sur le nombre d'attaques sont affichés.

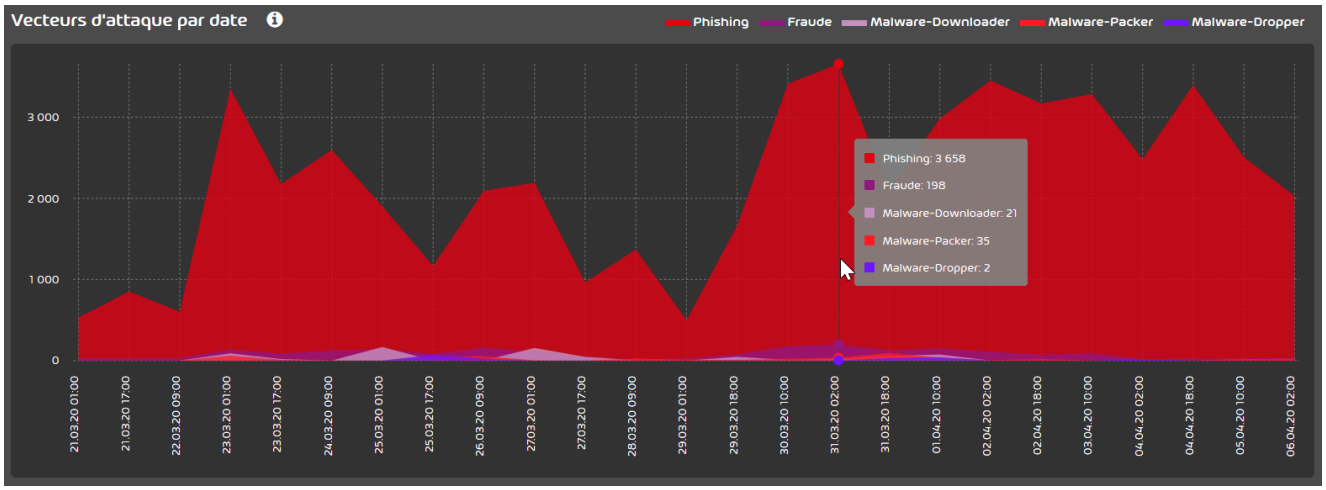


Illustration 148 : Statistiques des menaces - Vecteurs d’ attaque par date

Statistiques Secure Links

Les statistiques et diagrammes sous **Statistique de Secure Links** représentent le nombre de liens sur lesquels on a cliqué et qui ont été convertis en courriels par le moteur Secure-Link dans la période sélectionnée. Il s'agit de données globales pour tous les clients et non de données pour le domaine sélectionné. Les statistiques et diagrammes suivants sont affichés sous **Statistique de Secure Links** :

- La statistique **Clics par heure** montre la répartition de clics sur les liens dans les courriels en pourcentage.

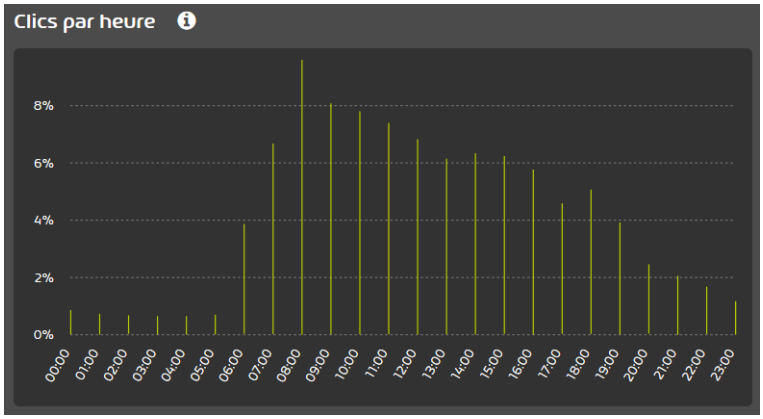


Illustration 149 : Clics par heure

- La statistique **Clics par appareil** montre la répartition de clics par appareil en pourcentage.

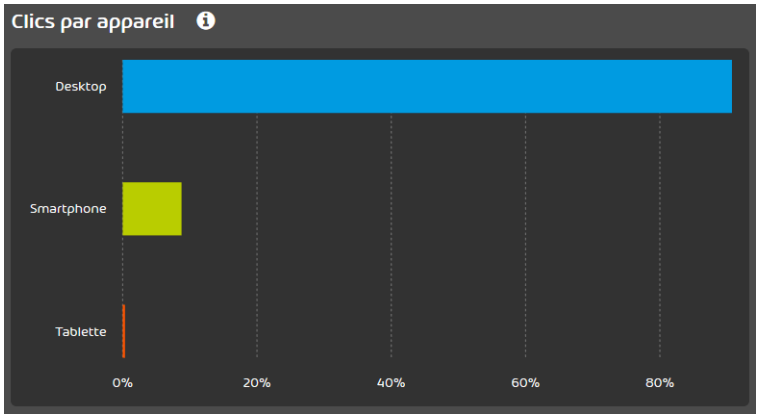


Illustration 150 : Clics par appareil

- Le diagramme **Clics par système d'exploitation (OS)** montre la répartition de clics par système d'exploitation en pourcentage.

Illustration 151 : Clics par système d’ exploitation (OS)

Types et vecteurs d’ attaque

Description des types d’ attaques

Tableau 10 : Types d’ attaque

NOM DU TYPE D’ ATTAQUE	EXPLICATION
Porte dérobée	Un maliciel de « porte dérobée » poursuit un objectif similaire à celui d'un cheval de Troie avec accès à distance, mais utilise une approche différente. Dans une attaque par porte dérobée, les attaquants utilisent ce qu'on appelle des « backdoor » ou portes dérobées, dont certaines ont été délibérément placées dans des programmes ou des systèmes d'exploitation. Cependant, il se peut qu'elles aient aussi été installées secrètement. La particularité des portes dérobées est qu'elles contournent les mécanismes de défense habituels et sont donc très attrayantes pour les cybercriminels, par exemple, elles sont très populaires pour la création de réseaux de bots.

NOM DU TYPE D'ATTAQUE	EXPLICATION
Cheval de Troie bancaire	Les chevaux de Troie bancaires sont un type maliciel qui tente de voler des données sensibles telles que des coordonnées bancaires ou des données de courriels. Les attaquants y parviennent souvent en combinaison avec des attaques de phishing, dans lesquelles un site Web prétend être un site Web officiel de la banque.
Bot	Un bot n'est pas forcément un maliciel. En effet, un bot est avant tout un programme informatique qui exécute des tâches indépendamment et automatiquement. Si plusieurs bots communiquent ensemble, on parle de réseau de bots. Les réseaux de bots sont de grandes collections d'ordinateurs infectés qu'un attaquant met en place. Un attaquant peut envoyer des commandes à tous les ordinateurs simultanément pour déclencher des activités. Ce qui est perfide, c'est que les propriétaires des ordinateurs ne remarquent pas « l'appartenance » à un réseau de bots avant que celui-ci n'ait déjà effectué les activités contrôlées de l'extérieur.
Crypto-mineur	Les crypto-mineurs sont une forme de maliciel utilisés pour calculer des devises numériques. Les criminels infectent les ordinateurs avec des crypto-mineurs pour tirer profit de leur puissance de calcul ou de l'utilisation de l'UC du cloud. Cela réduit la puissance de l'ordinateur ainsi que sa durée de vie. De plus, des réseaux d'entreprise entiers peuvent être arrêtés par des crypto-mineurs.
Keylogger	Les keyloggers sont un type de maliciels qui peuvent être implémentés à l'aide de matériel ou de logiciels. Les keyloggers enregistrent les frappes et la voix de l'utilisateur et peuvent ainsi accéder aux données sensibles ou aux mots de passe.

NOM DU TYPE D'ATTAQUE	EXPLICATION
Cheval de Troie de point de vente	Les chevaux de Troie de point de vente sont un type de maliciel qui attaque les systèmes de vente dans lesquels s'effectuent des transactions avec des données de paiement sensibles. Les cybercriminels utilisent des chevaux de Troie de point de vente pour accéder aux données non cryptées des clients provenant des cartes bancaires et de crédit.
Ransomware	Un ransomware fait référence aux attaques dans lesquelles les fichiers du système attaqué sont cryptés. Les fichiers ne peuvent pas être ouverts sans clé. Cependant, les attaquants exigent une rançon importante en échange de la clé. Même si un seul ordinateur est infecté au début, le ransomware peut se propager à l'ensemble du réseau.
Cheval de Troie avec accès à distance	Un cheval de Troie avec accès à distance (RAT) permet aux attaquants de prendre le contrôle des ordinateurs et de les contrôler à distance. Cela permet d'exécuter des commandes sur les systèmes de la victime et de répandre des RAT sur d'autres ordinateurs dans le but de construire un réseau de bots.
Root kit	Un root kit peut être utilisé pour empêcher de détecter un code malveillant. Dans cette forme d'attaque, l'attaquant pénètre profondément dans le système informatique, obtient les privilèges root et ainsi des droits d'accès généraux. Les cybercriminels modifient ensuite le système pour que l'utilisateur ne sache plus quand des processus et des activités sont lancés. Les attaques basées sur des dissimulations de root kits sont donc très difficiles à détecter.

NOM DU TYPE D' ATTAQUE	EXPLICATION
Logiciel espion	Un logiciel espion est un maliciel qui collecte des informations sur l'ordinateur de la victime. Ces informations peuvent être des données d'accès à des comptes utilisateurs, des données bancaires sensibles ou le comportement de navigation. Le plus souvent, les utilisateurs ne savent pas qu'ils ont été victimes d'un logiciel espion.
Chevaux de Troie	Les chevaux de Troie sont des programmes se voulant bienfaisant mais refermant un code malveillant. L'utilisateur ne détecte que l'application positive, tandis que l'exécution en arrière-plan du code malveillant infecte le système. À partir de ce moment, l'utilisateur ne peut plus influer sur les répercussions correspondantes.
Usurpation d' identité	Attaque par laquelle l'auteur usurpe l'identité d'une personne ou d'une entité en qui la victime a confiance ou qu'elle connaît, afin d'avoir accès à des informations sensibles, de voler de l'argent (par ex. en demandant un virement), d'accéder à la propriété intellectuelle, etc.

Description des vecteurs d' attaques

Tableau 11 : Vecteurs d' attaque

NOM DU VECTEUR D' ATTAQUE	EXPLICATION
Pièce-jointe	La pièce-jointe d'un courriel est un fichier qui peut contenir des maliciels.
Lien	Un lien dans un courriel est une mise en relation vers un autre site Web. Un maliciel peut se cacher derrière le lien.

NOM DU VECTEUR D'ATTAQUE	EXPLICATION
Link-Dropper	Les « Link-Dropper » sont des liens servant de support pour les maliciels. Le lien en soi n'est pas malveillant mais permet au maliciel qui se cache derrière de s'exécuter.
Link-Downloader	Les « Link-Downloader » sont des liens dans les courriels derrière lesquels un maliciel se trouve. Si la victime clique sur ce lien, le maliciel est téléchargé.
Malware-Downloader	Les « Malware-Downloader » sont classés dans les chevaux de Troie. En effet, ils téléchargent des fichiers malveillants secrètement à partir d'un serveur se trouvant à distance.
Malware-Dropper	Les « Malware-Dropper » ne sont pas des maliciels mais transportent des maliciels dans le système. De l'extérieur, le « Malware-Dropper » semble inoffensif et peut se camoufler sous forme de fichier. Les fichiers qu'il contient peuvent cependant s'exécuter tout seul et infecter le système avec des maliciels.
Malware-Packer	Les « Malware-Packer » sont un type de maliciel avec lequel les criminels compressent leurs maliciels avec une série de méthodes. Ils essaient ainsi de contourner les analyses de maliciels.
Fraude	La fraude du point de vue d'Internet désigne l'obtention de données sensibles, d'argent ou de données bancaires des utilisateurs à l'aide de services Internet. Par exemple, des sites Internet ou transactions peuvent se prétendre authentiques mais avoir été programmés en réalité par des cybercriminels. Une variante connue est la fraude au président : les criminels prétendent être des directeurs généraux et s'adressent par téléphone ou par courriel à la comptabilité d'une entreprise pour ordonner le virement de grosses sommes d'argent.

NOM DU VECTEUR D'ATTAQUE	EXPLICATION
Phishing	Phishing (hameçonnage) est composé des mots « password » (mot de passe) et « fishing » (pêcher) et signifie ainsi « pêcher des mots de passe ». Dans ce cadre, les cybercriminels font passer des courriels ou sites Web comme authentiques et incitent les utilisateurs à y saisir des données sensibles. Les utilisateurs donnent volontairement leurs données sans savoir qu'elles tombent alors entre les mains de criminels.

Actions dans le Threat Live Report

Basculer entre les données globales et les données spécifiques au domaine

Vous n'avez pas encore activé le bouton **global** dans **Threat Live Report**.

Dans la section **Vue d'ensemble des attaques en temps réel**, ainsi que dans les graphiques et statistiques sous **Attaques tentées** et **Statistiques des menaces**, vous pouvez choisir d'afficher les données globales pour tous les clients ou les données pour le domaine actuellement sélectionné dans la sélection de l'espace. Par défaut, l'affichage des données spécifiques au domaine est sélectionné.

REMARQUE :

Les graphiques sous **Statistique de Secure Links**, d'autre part, ne montrent que les données globales pour tous les clients, qui ne peuvent pas être basculées.

1. Sélectionnez un domaine dans la sélection de l'espace.

Le module **Threat Live Report** est activé sous **Rapports & conformité**.

2. Naviguez vers **Rapports & conformité** > **Threat Live Report**.

3. Actionnez le bouton **global**.

Illustration 152 : Bouton global sur fond vert

Le fond du bouton **global** devient vert. Les graphiques et les statistiques sous **Vue d'ensemble des attaques en temps réel**, **Attaques tentées** et **Statistiques des menaces** utilisent désormais des données globales pour tous les clients.

4. Actionnez à nouveau le bouton **global**.

Le fond du bouton **global** devient gris. Les graphiques et les statistiques de **Vue d'ensemble des attaques en temps réel**, **Attaques tentées** et **Statistiques des menaces** utilisent désormais les données du domaine sélectionné dans la sélection de l'espace.

L'affichage des graphiques et des statistiques sous **Threat Live Report** a été basculé des données globales aux données spécifiques au domaine (ou vice versa).

Sélectionner la période d'affichage

Vous pouvez sélectionner la période d'affichage des graphiques et des statistiques sous **Attaques tentées**, **Statistiques des menaces** et **Statistique de Secure Links**.

REMARQUE :

La section **Vue d'ensemble des attaques en temps réel** affiche toujours les données en temps réel et n'est pas affectée par la période sélectionnée.

1. Sélectionnez un domaine dans la sélection de l'espace.

Le module **Threat Live Report** est activé sous **Rapports & conformité**.

2. Naviguez vers **Rapports & conformité** > **Threat Live Report**.

3. Cliquez sur le bouton avec la période de temps.

Illustration 153 : Cliquez sur le bouton de sélection de la période

Un calendrier permettant de sélectionner des périodes de temps s'affiche.

4. Sélectionnez manuellement la période souhaitée.

   a) Cliquez sur le premier jour de la période souhaitée dans le calendrier.

   b) Cliquez sur le dernier jour de la période souhaitée.

La période souhaitée est sélectionnée.

Les graphiques et statistiques ci-dessus présentent les données de la période sélectionnée uniquement.

5. Sélectionnez une période de temps prédéfinie. Vous disposez des options suivantes :

   - **Aujourd'hui** : la période est limitée à aujourd'hui.
   - **Hier** : la période est limitée à la veille d'aujourd'hui.
   - **Il y a 2 jours** : la période est limitée au jour deux jours avant aujourd'hui.
   - **Ce mois-ci** : le mois civil en cours est sélectionné comme période.
   - **Le mois dernier** : le mois civil précédant le mois civil en cours est sélectionné comme période.
   - **Les 3 derniers mois** : le mois civil en cours et les deux mois civils précédents sont sélectionnés comme période.
   - **Cette année** : L'année civile en cours est sélectionnée comme période.
   - **Les 12 derniers mois** : Les 12 derniers mois sont sélectionnés comme période.

Les graphiques et statistiques ci-dessus présentent les données de la période sélectionnée uniquement.

La période d'affichage a été sélectionnée.

Audit 2.0

Auditing 2.0

Le module **Audit 2.0** permet de documenter les activités des utilisateurs du Control Panel dans un protocole d'audit. Dans le protocole d'audit, les administrateurs côté clients et côté partenaires peuvent suivre les activités de leurs utilisateurs. Les administrateurs peuvent par exemple déterminer quel utilisateur est responsable de la suppression d'un set de données et à quel moment cette action a été effectuée. Cela permet aux administrateurs d'annuler ces actions si nécessaire.

Chaque entrée de journal représente un événement qui a été réalisé par un utilisateur du Control Panel. Les informations sont enregistrées dans plusieurs catégories (voir Catégories à la page 188) pour chaque événement. Les administrateurs peuvent choisir lesquelles de ces catégories apparaîtront dans le protocole d'audit (voir Sélectionner les catégories affichées à la page 190).

Pour faciliter la recherche d'entrées, les administrateurs peuvent filtrer les entrées dans leprotocole d'audit. Les administrateurs peuvent définir la période pour laquelle les entrées apparaissent dans le protocole d'audit (voir Sélectionner la période d' affichage à la page 192). Les administrateurs peuvent également filtrer les entrées par actions (voir Filtrer par actions à la page 193) et événements (voir Filtrer par événements à la page 195). S'ils le souhaitent, les administrateurs peuvent réinitialiser les paramètres de filtre aux paramètres par défaut (voir Réinitialiser les paramètres à la page 206). En outre, les administrateurs peuvent effectuer des recherches par termes dans les entrées du protocole d'audit (voir Parcourir les entrées à la page 207).

Pour voir quelles valeurs ont été modifiées par un événement dans le Control Panel, les administrateurs peuvent ouvrir l'entrée de cet événement (voir Ouvrir une entrée à la page 208). En outre, les administrateurs peuvent exporter les entrées affichées au format CSV (voir Exporter des entrées à la page 210).

Catégories

Dans le module **Audit 2.0** (voir Auditing 2.0 à la page 188), les événements effectués par les utilisateurs du Control Panel sont documentés dans un protocole d'audit. Des informations sur plusieurs catégories sont enregistrées pour chaque entrée du protocole. Chaque colonne du

protocole d'audit correspond à une catégorie. Les catégories sont expliquées dans le tableau ci-dessous.

Tableau 12 : Catégories dans le protocole d' audit

CATÉGORIE	EXPLICATION
Horodatage	Montre l'heure de l'action exécutée.
Utilisateur	Indique l'utilisateur qui a exécuté l'action.
Cible	Indique l'utilisateur pour lequel l'action a été exécutée.
Événement	Indique de quel événement il s'agit, par ex. d'une modification des paramètres utilisateur, de la Blacklist ou de la Whitelist, des identifiants ou d'une connexion.
Action	Indique si l'action exécutée a créé, actualisé ou supprimé quelque chose. Réussite ou Erreur indiquent si une connexion a réussi.
Chemin cible	Indique dans quel domaine l'utilisateur cible pour lequel l'action a été exécutée est créé.
ID de l'application	Indique les numéros d'identification des applications qui utilisent l'API. Via l'API, les applications peuvent communiquer avec nos services. Pour de plus amples informations sur l'API, voir les instructions « Application Programming Interface (API) ».
Version de l'application	Indique la version de l'application qui a communiqué avec l'API.
IP	Indique l'adresse IPv4 de l'utilisateur qui a exécuté l'action.

CATÉGORIE	EXPLICATION
URL	Indique le chemin vers le point final de l'API.

Les catégories suivantes sont affichées par défaut dans le protocolle d'audit :

- **Horodatage**
- **Utilisateur**
- **Cible**
- **Événement**
- **Action**

En outre, les administrateurs peuvent afficher les catégories suivantes dans le protocole d'audit (voir Sélectionner les catégories affichées à la page 190) :

- **Chemin cible**
- **ID de l'application**
- **Version de l'application**
- **IP**
- **URL**

Sélectionner les catégories affichées

Le protocole d'audit dans le module **Audit 2.0** (voir Auditing 2.0 à la page 188) contient des informations concernant les différentes catégories (voir Catégories à la page 188). Vous pouvez sélectionner les catégories qui seront affichées dans le protocole d'audit. Chaque colonne du protocole d'audit correspond à une catégorie.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client dont vous souhaitez ouvrir le protocole d'audit.
3. Naviguez vers **Rapports & conformité** > **Audit 2.0**.

4. Cliquez sur le bouton en haut à droite du tableau.

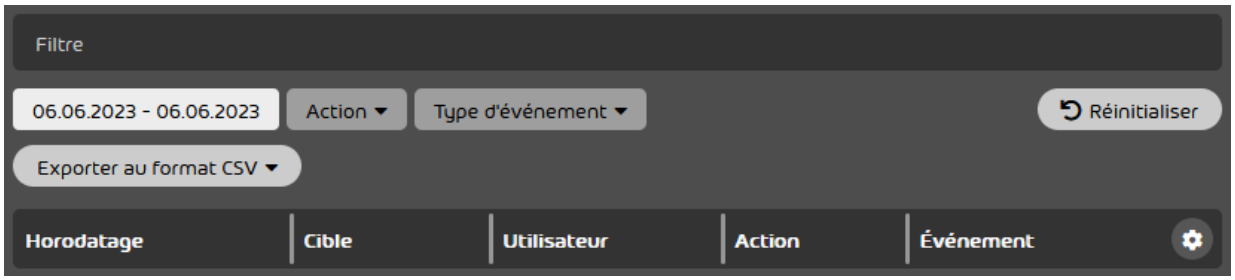


Illustration 154 : Ouvrir la vue d' ensemble des catégories disponibles

Une liste de toutes les catégories disponibles apparaît. Le fond des catégories actuellement affichées dans le protocole d'audit est vert.

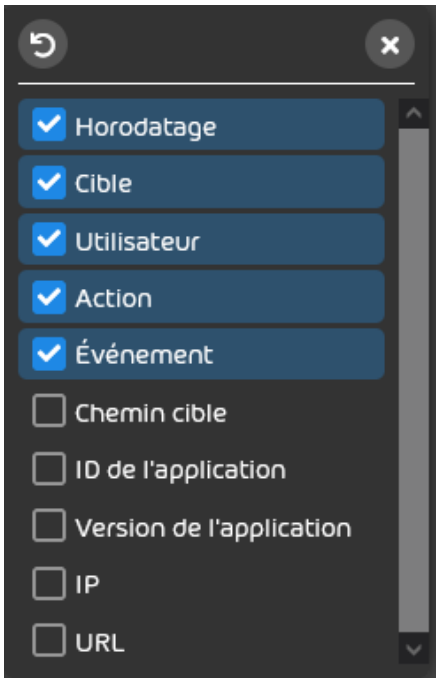


Illustration 155 : Catégories disponibles

5. Pour afficher une catégorie actuellement non affichée dans le protocole d'audit, cliquez sur la catégorie.

Le fond de la catégorie devient vert.

6. Pour masquer une catégorie actuellement affichée dans le protocole d'audit, cliquez sur la catégorie.

➔ Le fond de la catégorie n'est plus en vert.

7. Facultatif : Pour réinitialiser les colonnes du tableau du protocole d'audit à leurs paramètres par défaut, cliquez sur **Default**.

➔ Les colonnes du tableau du protocole d'audit sont réinitialisées à leurs paramètres par défaut.

8. Cliquez dans la fenêtre en dehors de la liste pour la fermer.

➔ La liste est fermée. Les catégories sélectionnées apparaissent dans le protocole d'audit.

✔ Les catégories pour l'affichage dans le protocole d'audit ont été sélectionnées.

Filtrage des entrées

Sélectionner la période d' affichage

Le module **Audit 2.0** (voir Auditing 2.0 à la page 188) vous permet de sélectionner une période d'affichage pour le protocole d'audit.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client dont vous souhaitez ouvrir le protocole d'audit.
3. Naviguez vers **Rapports & conformité** > **Audit 2.0**.
4. Cliquez sur la plage de dates affichée.

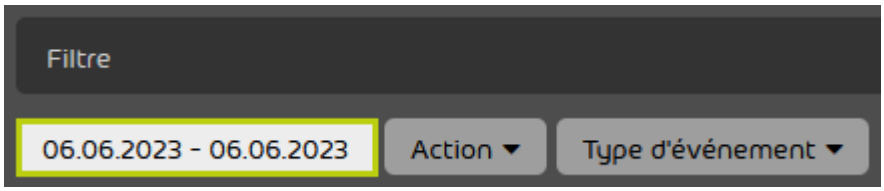


Illustration 156 : Sélectionner une période

➔ Un calendrier s'ouvre.

5. Dans le calendrier, sélectionnez la période pendant laquelle les événements doivent être affichés dans le protocole d'audit.

   Tous les jours de la période sélectionnée sont marqués dans le calendrier. La date de début et la date de fin sont affichées sous le calendrier.

6. Cliquez dans la fenêtre à l'extérieur du calendrier pour fermer ce dernier.

   Le calendrier est fermé. Le protocole d'audit n'affiche que les événements de la période sélectionnée.

Une période d'affichage a été sélectionnée pour le protocole d'audit.

Filtrer par actions

Actions filtrables

Les administrateurs peuvent filtrer les entrées du protocole d'audit dans le module **Audit 2.0** (voir Auditing 2.0 à la page 188) par actions. Pour cela, les administrateurs peuvent choisir une action dans le menu déroulant **Action**. Après la sélection, seules les entrées de l'action sélectionnée sont affichées.

REMARQUE :

Il n'est possible de filtrer qu'une seule action à la fois.

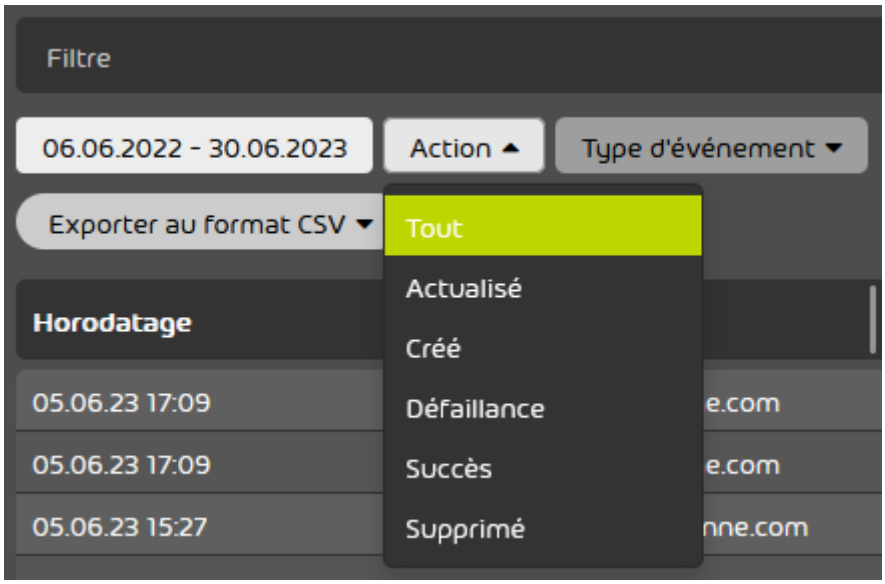


Illustration 157 : Filtrer par actions

Dans le tableau suivant, les actions que les administrateurs peuvent filtrer sont listées.

Tableau 13 : Actions

ACTION	EXPLICATION
Tout	Montre toutes les actions qui se sont produites dans la période indiquée.
Actualisé	Montre toutes les actions qui ont actualisé quelque chose.
Succès	Montre toutes les connexions qui ont réussi.
Créé	Montre toutes les actions qui ont créé quelque chose.
Défaillance	Montre toutes les tentatives de connexion qui ont échoué.
Supprimé	Montre toutes les actions qui ont supprimé quelque chose.

Filtrer par événements

Événements filtrables

Les administrateurs peuvent filtrer les entrées du protocole d'audit dans le module **Audit 2.0** (voir Auditing 2.0 à la page 188) par événements. Dans le menu déroulant **Type d'événement**, les administrateurs peuvent sélectionner un événement. Dès qu'un un événement a été sélectionné, seules les entrées relatives à cet événement s'affichent.

REMARQUE :

Il n'est possible de filtrer qu'un seul événement à la fois.

Le module **Audit 2.0** permet aux administrateurs de voir tous les événements qui ont été exécutés au niveau du partenaire ou du client actuellement sélectionné ainsi que de tous les domaines d'application subordonnés. Les entrées pour l'événement **Action sur le courriel** sont auditées au niveau du domaine d'application le plus élevé auquel l'utilisateur qui a exécuté l'événement a accès.

REMARQUE :

À l'exception de l'événement **Action sur le courriel**, toutes les entrées sont auditées au niveau du domaine d'application sélectionné dans la sélection de l'espace lors de l'exécution de l'événement (voir le chapitre « Sélection de l'espace » dans le manuel du Control Panel).

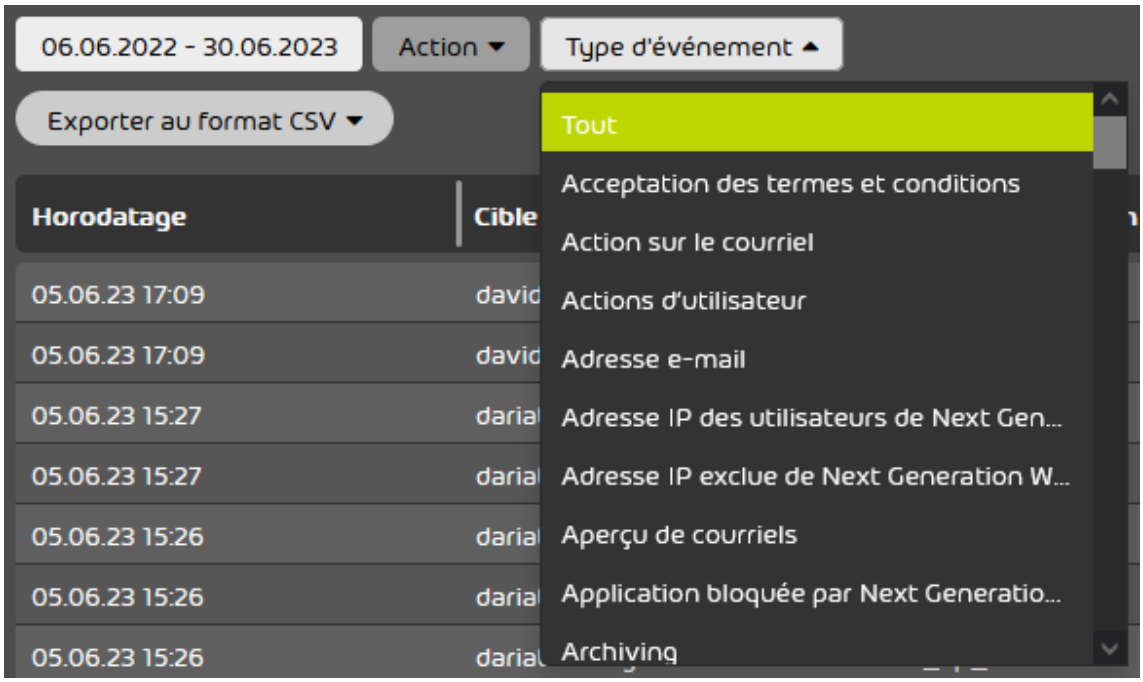


Illustration 158 : Filtrer par événement

Dans le tableau suivant, les événements que les administrateurs peuvent filtrer sont listés.

Tableau 14 : Événements filtrables

ÉVÉNEMENT	EXPLICATION
Tout	Affiche toutes les modifications dans le Control Panel.
Paramètres généraux LDAP	Filtre les événements qui ont entraîné la mise à jour des paramètres généraux pour toutes les connexions LDAP du module **Tableau de bord des services**.
Message d'absence	Filtre les événements qui ont entraîné une mise à jour des paramètres de la note d'absence dans le module **Paramètres utilisateur**.

ÉVÉNEMENT	EXPLICATION
Données de connexion	Filtre les événements qui ont entraîné une mise à jour des identifiants d'un utilisateur.
Connexion	Filtre les connexions réussies et échouées dans le Control Panel.
Jeton d'API	Filtre les événements qui ont entraîné la création ou la suppression de jetons d'API dans l'onglet **Jeton d'API** sous **Paramètres utilisateur**.
Configuration ATP	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Advanced Threat Protection**.
Aspect	Filtre les événements qui ont entraîné une mise à jour des paramètres dans l'onglet **Control Panel** dans le module **Personnalisation**.
Aspect des rapports de quarantaine	Filtre les événements qui ont entraîné une mise à jour de l'apparence des rapports de quarantaine. En font notamment partie les modifications dans les modules **Personnalisation** et **Quarantine Report**.
Déconnexion automatique : configuration	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des paramètres personnalisés pour la déconnexion automatique des utilisateurs inactifs dans le module **Paramètres client** > **Authentification**.

ÉVÉNEMENT	EXPLICATION
Création automatique d'utilisateurs	Filtre par événements qui ont entraîné l'actualisation de l'état d'activation de l'option pour la création automatique d'utilisateurs en fonction de la méthode de vérification des utilisateurs dans le module **Spam and Malware Protection**.
Sauvegarde	Filtre les événements qui ont entraîné l'activation des services de sauvegarde et de restauration des données.
Actions d' utilisateur	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des paramètres des actions autorisées dans l'onglet **Droits d' utilisateurs** dans le module **Spam and Malware Protection**.
Paramètres utilisateur	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des paramètres sous **Paramètres utilisateur**. Les modifications apportées aux valeurs par défaut du fuseau horaire, de la langue, du format de date et d'heure d'un partenaire ou d'un client dans le module **Tableau de bord des services** (voir le chapitre « Régler les valeurs par défaut pour le fuseau horaire et la langue » dans le manuel Control Panel) sont également auditées sous cet événement.
Expéditeurs interdits et autorisés	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Expéditeurs interdits et autorisés**.

ÉVÉNEMENT	EXPLICATION
Compliance Filter	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression de règles, ainsi que la mise à jour des paramètres dans le module **Compliance Filter**.
Installation du connecteur	Filtre les événements qui ont entraîné l'installation des connecteurs.
Content Control	Filtre les événements qui ont entraîné la création et la mise à jour des paramètres dans le module **Content Control**.
Continuity Service	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Continuity Service**.
Domaine	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des domaines dans le module **Domaines**.
Adresse e-mail	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression d'adresses courriel dans le module **Boîtes aux lettres**.

ÉVÉNEMENT	EXPLICATION
Action sur le courriel	Filtre les événements liés aux actions sur les courriels dans le module **Email Live Tracking**. Les actions sur les courriels suivantes reçoivent le statut **Actualisé** : • **Signaler un spam** • **Signaler un infomail** • **Marquer comme confidentiel** L'action sur les courriels **Supprimer le courriel** reçoit le statut **Supprimé**. Les actions sur les courriels suivantes reçoivent le statut **Succès** : • **Libérer le courriel** • **Interdire l'expéditeur** • **Autoriser l'expéditeur et libérer le courriel** • **Interdire l'expéditeur pour tous les utilisateurs** • **Autoriser l'expéditeur pour tous les utilisateurs** • **Courriel à admin** • **Scan ATP**
Informations des courriels	Filtre les événements qui ont entraîné une mise à jour des paramètres dans l'onglet **Informations des courriels** dans le module **Personnalisation**.

ÉVÉNEMENT	EXPLICATION
Destinataires des statistiques des courriels	Filtre les événements qui ont entraîné l'ajout ou la suppression de boîtes aux lettres dans la liste des destinataires des statistiques de courriels dans le module **Statistiques des courriels**.
Aperçu de courriels	Filtre les événements qui ont entraîné la création d'une prévisualisation du courriel dans le module **Email Live Tracking**.
Email Authentication	Filtre les événements qui ont entraîné la création ou la suppression d'exceptions, et la mise à jour des paramètres dans le module **Email Authentication**.
Termes et conditions	Filtre les événements qui ont entraîné la création ou la mise à jour des paramètres dans l'onglet **Termes et conditions** dans le module **Tableau de bord des services**.
Groupe	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression de groupes dans le module **Groupes**.
Contenu des termes et conditions	Filtre les événements qui ont entraîné la création d'un texte du contrat de licence d'utilisateur final et du contrat de traitement des données dans l'onglet **Termes et conditions** du module **Tableau de bord des services**.
Contact	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression de contacts dans le module **Tableau de bord des services**.

ÉVÉNEMENT	EXPLICATION
Client	Filtre les événements qui ont entraîné la création ou la suppression de clients dans le module **Tableau de bord des services**.
Connexion LDAP	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des paramètres d'une connexion LDAP dans le module **Tableau de bord des services**.
Migration d' une seule boîte aux lettres	Filtre les événements qui ont entraîné la mise à jour ou la suppression d'une tâche de migration des données d'une seule boîte aux lettres lors de la migration de boîte aux lettres dans le module **365 Total Protection**.
Migration de plusieurs boîtes aux lettres	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression d'une tâche de migration des données de plusieurs boîtes aux lettres pendant la migration de boîte aux lettres dans le module **365 Total Protection**.

ÉVÉNEMENT	EXPLICATION
Authentification multifacteur	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des paramètres de l'authentification multifacteur. La création signifie que l'authentification multifacteur a été activée pour les utilisateurs d'un domaine dans le module **Paramètres client** > **Authentification**. La mise à jour signifie qu'un utilisateur a configuré l'authentification multifacteur sous **Paramètres utilisateur** pour son propre compte. La suppression signifie qu'un utilisateur a désactivé l'authentification multifacteur pour son propre compte sous **Paramètres utilisateur**, qu'un administrateur a réinitialisé l'authentification multifacteur pour un utilisateur dans le module **Paramètres client** > **Boîtes aux lettres** ou qu'un administrateur a désactivé l'authentification multifacteur pour les utilisateurs d'un domaine dans le module **Paramètres client** > **Authentification**.
Bulletin	Filtre les événements qui ont entraîné l'abonnement aux newsletters pour les clients ou partenaires dans le module **Tableau de bord des services**.
Mot de passe d' urgence de l' utilisateur	Filtre les événements qui ont entraîné la mise à jour du mot de passe d'urgence pour le Continuity Service.
Outlook Add-in	Filtre les événements qui ont entraîné une mise à jour des paramètres dans l'add-in Outlook.

ÉVÉNEMENT	EXPLICATION
Partenaire	Filtre les événements qui ont entraîné la création ou la suppression de partenaires dans le module **Tableau de bord des services**.
Politique de mot de passe	Filtre les événements qui ont entraîné la mise à jour des préférences en matière de mot de passe dans le module **Authentification**.
Boîte aux lettres	Filtre les événements qui ont entraîné la création ou la mise à jour de boîtes aux lettres dans le module **Boîtes aux lettres**.
Quarantine Report	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Quarantine Report**.
Attribution de rôles	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression d'attributions de rôles dans le module **Tableau de bord des services**.
Spam and Malware Protection	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Spam and Malware Protection**.
Informations du support	Filtre les événements qui ont entraîné une mise à jour des paramètres dans l'onglet **Informations du support** dans le module **Personnalisation**.

ÉVÉNEMENT	EXPLICATION
Groupes de Targeted Fraud Forensics Filter	Filtre les événements qui ont entraîné la création ou la suppression de groupes pour le Targeted Fraud Forensics Filter dans le module **Advanced Threat Protection**.
Environnement	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression d'environnements secondaires dans le module **Tableau de bord des services**.
Validation d' environnment	Filtre les événements qui ont entraîné la création ou la suppression de la validation d'un environnement pour la migration de boîte aux lettres dans le module **365 Total Protection**.
Attribution d'environnements	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des attributions d'environnements aux boîtes aux lettres dans le module **Paramètres client** > **Boîtes aux lettres**. Le terme « création » signifie qu'un environnement a été attribué pour la première fois à une boîte aux lettres qui vient d'être créée. Le terme « mise à jour » signifie qu'un environnement différent du précédent a été attribué à une boîte aux lettres. Le terme « suppression » signifie que la suppression d'une boîte aux lettres a entraîné la suppression de son affectation à un environnement.
Dictionnaire du Compliance Filter	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression de dictionnaires dans le module **Compliance Filter**.

ÉVÉNEMENT	EXPLICATION
Directives	Filtre les événements qui ont entraîné une mise à jour des paramètres dans le module **Authentification**.
Identifiants pour la migration de boîte aux lettres	Filtre les événements qui ont entraîné la création ou la suppression des identifiants d'un serveur Exchange local pour la migration de boîte aux lettres dans le module **365 Total Protection**.

Événements supplémentaires

Le tableau suivant énumère les événements que les administrateurs ne peuvent pas filtrer, mais qui sont tout de même affichés dans le module **Audit 2.0**.

Tableau 15 : Événements non filtrables

ÉVÉNEMENT	EXPLICATION
Données de base	Filtre les événements qui ont entraîné la création, la mise à jour ou la suppression des données de base des boîtes aux lettres dans le module **Boîtes aux lettres**.

Réinitialiser les paramètres

Vous avez modifié les paramètres d'affichage du protocole d'audit dans le module **Audit 2.0** (voir Sélectionner la période d' affichage à la page 192, Filtrer par actions à la page 193 et Filtrer par événements à la page 195). Vous vous trouvez toujours dans le module **Audit 2.0**.

Le module **Audit 2.0** vous permet de réinitialiser les paramètres d'affichage du protocolle d'audit (voir Auditing 2.0 à la page 188) aux paramètres standard.

Cliquez sur **Réinitialiser**.

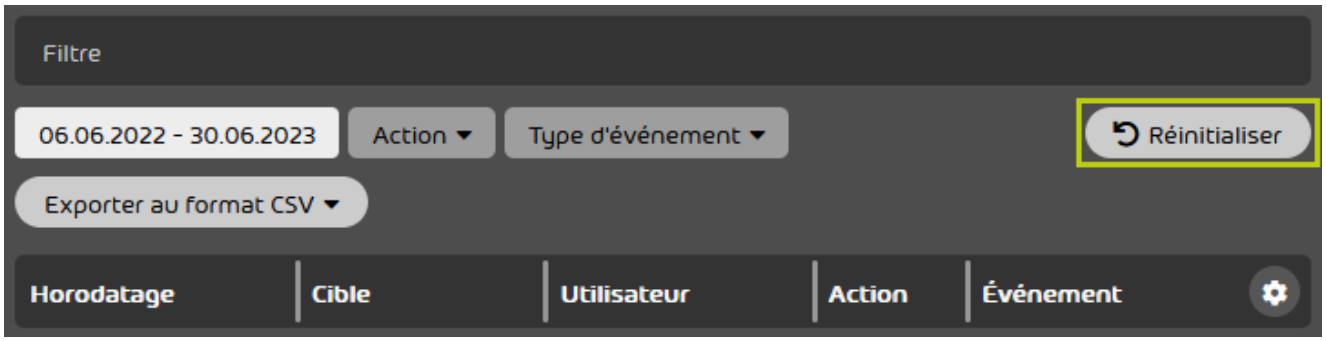


Illustration 159 : Réinitialiser aux paramètres par défaut

Les paramètres sont réinitialisés.

Les paramètres d'affichage du protocolle d'audit ont été réinitialisés aux paramètres standard.

Parcourir les entrées

Dans le module **Audit 2.0** (siehe Auditing 2.0 à la page 188), les administrateurs peuvent rechercher par termes les entrées du protocole d'audit. Pour cela, les administrateurs peuvent rechercher par termes dans les paramètres suivants :

- **Utilisateur**
- **Chemin cible**
- **Cible**
- **ID de l'application**
- **Version de l'application**
- **Anciennes valeurs**
- **Nouvelles valeurs**
- **IP**
- **URL**

Tous les paramètres, à l'exception des paramètres **Anciennes valeurs** et **Nouvelles valeurs** correspondent à des catégories du protocole d'audit (voir Catégories à la page 188). Les paramètres **Anciennes valeurs** et **Nouvelles valeurs** quant à eux se réfèrent aux anciennes et aux nouvelles valeurs enregistrées dans les entrées du protocole d'audit sous le point de menu **Info**.

Les administrateurs peuvent saisir un terme de recherche dans la barre de recherche. Pour rechercher un paramètre spécifique à partir du terme de recherche, les administrateurs peuvent ensuite cliquer sur le paramètre souhaité sous la barre de recherche. Si ce n'est pas le cas, tous les paramètres seront recherchés en fonction du terme de recherche. Les administrateurs peuvent lancer la recherche en appuyant sur la touche « Entrée ». Seules les entrées qui répondent aux critères de recherche apparaissent dans le protocole d'audit.

REMARQUE :

Les administrateurs peuvent utiliser plusieurs paramètres en même temps. Les administrateurs peuvent saisir un terme de recherche pour chaque paramètre utilisé. Les résultats de recherche contiennent uniquement des entrées qui répondent à tous les critères de recherche.

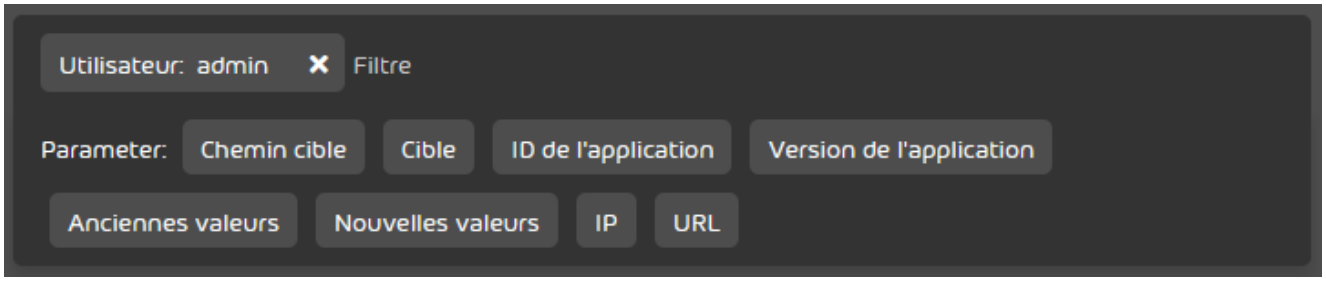


Illustration 160 : Parcourir les entrées

Ouvrir une entrée

Vous pouvez ouvrir une entrée du protocole d'audit dans le module **Audit 2.0** pour voir quelles valeurs étaient valables avant et après un événement.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le client dont vous souhaitez ouvrir le protocole d'audit.
3. Naviguez vers **Rapports & conformité** > **Audit 2.0**.
4. Facultatif : Pour rechercher une entrée, filtrez les entrées du protocole d'audit (voir Sélectionner la période d' affichage à la page 192, Filtrer par actions à la page 193, Filtrer par événements à la page 195 ou Parcourir les entrées à la page 207).
5. Cliquez sur la flèche de menu à côté de l'entrée que vous souhaitez ouvrir.

Illustration 161 : Ouvrir le menu

- Un menu s'ouvre.

6. Cliquez sur **Info**.

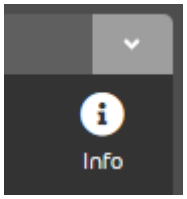


Illustration 162 : Ouvrir les informations

- L'entrée est ouverte. Si elles existent, les anciennes et les nouvelles valeurs de l'événement sont affichées.

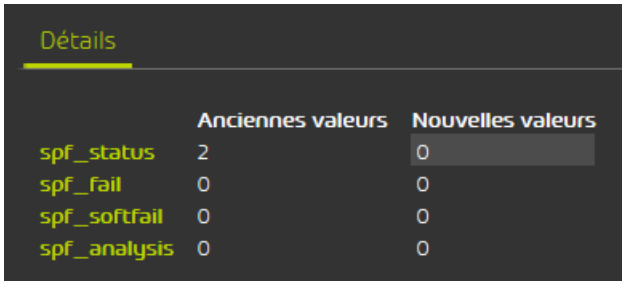


Illustration 163 : Valeurs de l' événement

REMARQUE :

La valeur qui a été modifiée par l'événement se trouve sur fond gris.

Une entrée du protocole d'audit a été ouverte.

Exporter des entrées

Dans le module **Audit 2.0** (voir Auditing 2.0 à la page 188), vous pouvez exporter les entrées du protocole d'audit sous forme de fichier CSV. Lors de l'exportation, toutes les entrées affichées dans le module **Audit 2.0** sont exportées. Vous pouvez sélectionner les colonnes à partir desquelles les données seront exportées.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client dont vous souhaitez ouvrir le protocole d'audit.
3. Naviguez vers **Rapports & conformité** > **Audit 2.0**.
4. Sélectionnez comme période d'affichage la période dont les entrées doivent être exportées (voir Sélectionner la période d' affichage à la page 192).
5. Filtrez les entrées affichées par action (voir Filtrer par actions à la page 193).
6. Filtrez les entrées affichées par événement (voir Filtrer par événements à la page 195).
7. Cliquez sur **Exporter au format CSV**.

Un formulaire d'exportation des entrées du protocole d'audit.

Illustration 164 : Formulaire

8. Cochez les cases des catégories dont vous souhaitez exporter les données du protocole d'audit. Vous avez les options suivantes :

   - **Horodatage**
   - **Utilisateur**
   - **Chemin cible**
   - **Cible**
   - **ID de l'application**
   - **Version de l'application**
   - **IP**
   - **Action**
   - **Événement**
   - **URL**

> **REMARQUE :**
>
> Chaque catégorie correspond à une colonne du protocole d'audit (voir Catégories à la page 188). Par défaut, toutes les catégories sont présélectionnées dans le formulaire.

9. Sous **Type d'exportation**, indiquez si le fichier CSV doit être mis à disposition en téléchargement ou envoyé par courriel.
   - **Téléchargement** : le fichier CSV est mis à disposition dans les téléchargements.
   - **Par courriel** : le fichier CSV est envoyé par courriel.

Illustration 165 : Sélectionner le type d'exportation

Si l'option **Par courriel** a été sélectionnée, un champ supplémentaire s'affiche.

10. Facultatif : Si vous avez sélectionné l'option **Par courriel**, saisissez l'adresse courriel à laquelle le fichier CSV doit être envoyé dans le champ.

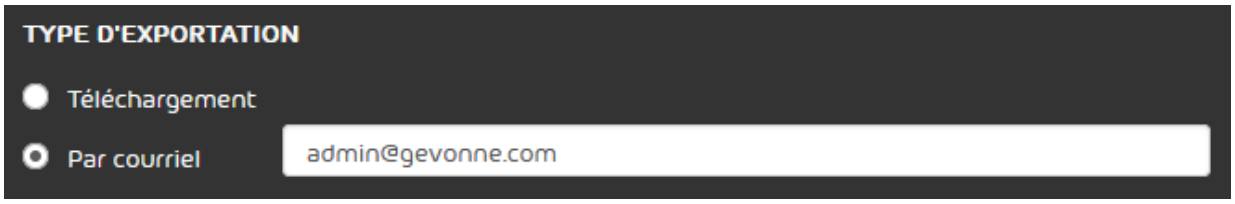


Illustration 166 : Saisir l'adresse courriel

11. Cliquez sur **Exporter**.

Le fichier CSV est mis à disposition dans les téléchargements ou envoyé par courriel.

Les entrées du protocole d'audit ont été exportées.

Paramètres des clients

Paramètres des clients

Dans le module **Paramètres client**, les administrateurs côté clients peuvent afficher et gérer les paramètres de base des boîtes aux lettres, groupes, domaines ainsi que les politiques de mots de passe et adresses IP. Le module **Paramètres client** est divisé dans les sous-modules suivants :

- **Boîtes aux lettres** : Les utilisateurs dans le Control Panel sont gérés via des boîtes aux lettres. Afin que nos services puissent être appliqués aux boîtes aux lettres, ceux-ci doivent être enregistrés dans le Control Panel. Dans ce module, les administrateurs côté clients peuvent ajouter les boîtes aux lettres de leurs domaines au Control Panel et gérer les boîtes aux lettres (voir Boîtes aux lettres à la page 213).
- **Groupes** : Les boîtes aux lettres peuvent être regroupées en groupes dans le Control Panel afin de pouvoir effectuer des configurations de groupes pour différents services. Dans ce module, les administrateurs côté clients peuvent créer et gérer des groupes (voir Groupes à la page 268).
- **Domaines** : Dans le Control Panel, des domaines d'alias peuvent être ajoutés à un domaine principal afin que les boîtes aux lettres des domaines d'alias puissent également être ajoutées au Control Panel. Dans ce module, les administrateurs côté clients peuvent ajouter, exporter et supprimer des domaines d'alias dans le Control Panel (voir Domaines à la page 285).
- **Authentification** : Ce module permet aux administrateurs côté clients d'effectuer des réglages pour l'authentification d'utilisateurs dans le Control Panel (voir Authentification à la page 297).

Boîtes aux lettres

Le module **Paramètres client** > **Boîtes aux lettres** permet d'afficher et de gérer toutes les boîtes aux lettres enregistrées qui sont subordonnées au domaine sélectionné. Ce module est disponible uniquement pour les administrateurs côté clients.

Les boîtes aux lettres constituent la base de licence pour tous les services. Une boîte aux lettres principale représente alors un seul utilisateur. En plus d'une boîte aux lettres principale, il est possible

de créer plusieurs adresses alias associées pour lesquelles aucun frais n'est facturé (voir Ajouter une adresse alias à la page 243).

Afin de pouvoir utiliser nos services pour une boîte aux lettres, celle-ci doit être présente dans le Control Panel. Les administrateurs côté clients peuvent ajouter des boîtes aux lettres individuelles au Control Panel (voir Ajouter une boîte aux lettres à la page 220) ou importer plusieurs boîtes aux lettres à partir d'un fichier CSV (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227) dans le Control Panel (voir Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223). Les boîtes aux lettres peuvent aussi être automatiquement ajoutées au Control Panel (voir Création automatique de boites aux lettres à la page 219).

En outre, les administrateurs côté clients peuvent créer des boîtes aux lettres de redirection (voir Ajouter boîte aux lettres de redirection à la page 237) pour lesquelles les courriels entrants seront redirigés vers d'autres boîtes aux lettres (voir Types de boîtes aux lettres à la page 218). Les destinataires des boîtes aux lettres de redirection peuvent être importés à partir d'un fichier CSV (voir Fichiers CSV pour l' importation de destinataires pour les boîtes aux lettres de redirection à la page 249).

Les boîtes aux lettres du Control Panel peuvent être exportées sous forme de fichier CSV (voir Exporter des boîtes aux lettres sous un fichier CSV à la page 234) et être réimportées dans le Control Panel par la suite via l'importation CSV.

Si nos services ne doivent plus être appliqués à une ou plusieurs boîtes aux lettres, celles-ci peuvent être supprimées du Control Panel (voir Supprimer une boîte aux lettres à la page 262 et Supprimer plusieurs boîtes aux lettres à la page 265).

Les boîtes aux lettres existantes peuvent être triées dans le module **Boîtes aux lettres** en fonction de leur type et de leur environnement (voir Configuration d' environnement principal à la page 456 et Environnements secondaires à la page 113). Les boîtes aux lettres peuvent être filtrées par type dans le menu déroulant **Tous les types** (voir Types de boîtes aux lettres à la page 218).

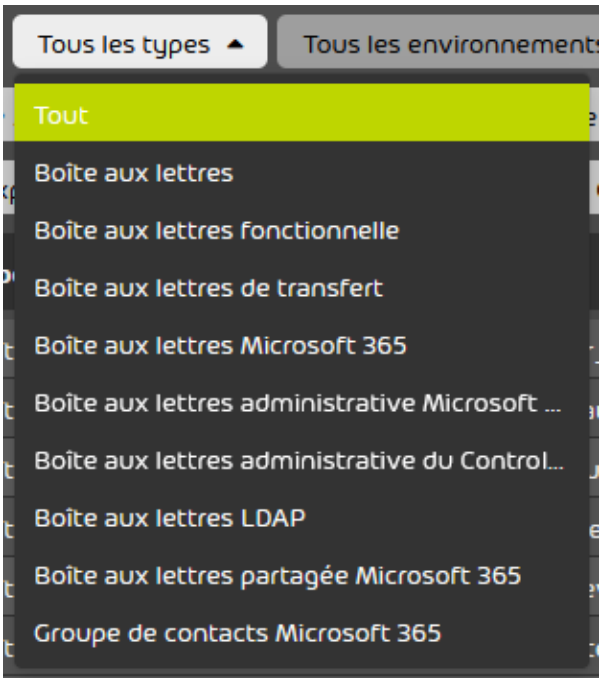


Illustration 167 : Filtrage par type

Les boîtes aux lettres peuvent être filtrés par environnement dans le menu déroulant **Tous les environnements**. L'environnement principal et les environnements secondaires du domaine sont indiqués dans le menu déroulant.

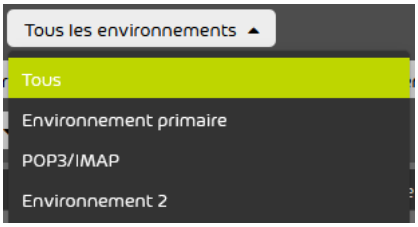


Illustration 168 : Filtrage par environnement

Le menu déroulant **Authentification multifacteur** apparaît uniquement si un administrateur côté client a activé l'authentification multi-facteurs pour les boîtes aux lettres du client (voir Activer l'authentification multifacteur à la page 301). Dans ce menu déroulant, les boîtes aux lettres peuvent être filtrées selon leur configuration d'authentification multi-facteurs.

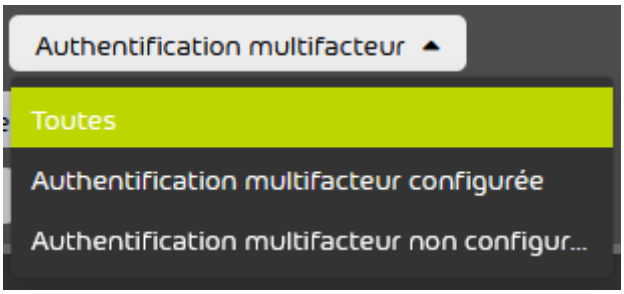


Illustration 169 : Filtrage par authentification multifacteur

En outre, le module **Boîtes aux lettres** propose aux administrateurs côté clients les options suivantes dans le menu des boîtes aux lettres afin de gérer les différentes boîtes aux lettres.

Tableau 16 : Gérer les boîtes aux lettres

SYMBOLE	DÉSIGNATION	DESCRIPTION
	Groupes	Ajouter la boîte aux lettres à un groupe (voir Groupes à la page 268 et Ajouter une boîte aux lettres à un groupe à la page 239) et supprimer la boîte aux lettres d'un groupe (voir Supprimer une boîte aux lettres d'un groupe à la page 241)
	Fuseau horaire et langue	Modification du fuseau horaire, de la langue, du format de date et du format d'heure de la boîte aux lettres (voir Définir le fuseau horaire et la langue d'une boîte aux lettres à la page 250)
	Données de base	Modification des données de base de la boîte aux lettres (voir Éditer des données de base d'une boîte aux lettres à la page 252)
	Changer environnement	Modification de l'environnement de la boîte aux lettres (voir Modifier l'environnement à la page 257)
	Changer mot de passe	Modification du mot de passe (voir Modifier le mot de passe à la page 259)

SYMBOLE	DÉSIGNATION	DESCRIPTION
	Réinitialiser l'authentification multifacteur	Réinitialisation de l'authentification multifacteur pour la boîte aux lettres (voir Réinitialiser l'authentification multifacteur à la page 261) **REMARQUE :** Cette action est visible uniquement si l'authentification multi-facteurs est activée pour le domaine (voir Activer l'authentification multifacteur à la page 301).
	Actif ou **Inactif**	Activation ou désactivation de la boîte aux lettres (voir Activer ou désactiver une boîte aux lettres à la page 242)
	Alias	Ajout d'une adresse alias à une boîte aux lettres principale (voir Ajouter une adresse alias à la page 243)
	Délégué	Saisie d'une délégation pour la boîte aux lettres (voir Saisir une délégation à la page 245)
	Quarantine Report	Configuration du Quarantine Report pour la boîte aux lettres (voir Configurer le Quarantine Report pour une boîte aux lettres à la page 436)
	Éliminer	Suppression de la boîte aux lettres (voir Supprimer une boîte aux lettres à la page 262)

REMARQUE :

Certaines des fonctions décrites ne peuvent pas être appliquées aux aux boîtes aux lettres LDAP, ou seulement de façon limitée. Il y est fait référence dans les chapitres des fonctions concernées.

Types de boîtes aux lettres

Le Control Panel fait la différentece entre les types de boîtes aux lettres suivants :

Tableau 17 : Types de boîtes aux lettres

TYPE DE BOÎTES AUX LETTRES	EXPLICATION
Boîte aux lettres	Cette boîte aux lettres a été créée manuellement dans le Control Panel. La boîte aux lettres n'est pas synchronisée avec un service d'annuaire via LDAP. Pour de plus amples informations sur la création de boîtes aux lettres de ce type, voir Ajouter une boîte aux lettres à la page 220.
Boîte aux lettres fonctionnelle	Les boîtes aux lettres de ce type ne sont actuellement pas enregistrées dans le Control Panel.
Boîte aux lettres de transfert	Une boîte aux lettres de renvoi est une boîte aux lettres virtuelle liée à au moins une boîte aux lettres dans le Control Panel ou à une boîte aux lettres externe. Les courriels entrants de la boîte aux lettres de redirection sont transférés vers ses boîtes aux lettres liées. Pour de plus amples informations sur la création de boîtes aux lettres de redirection, voir Ajouter boîte aux lettres de redirection à la page 237.
Boîte aux lettres administrative du Control Panel	Le rôle **admin** est attribué aux boîtes aux lettres de ce type dans le Control Panel (voir le chapitre « Rôles » dans le manuel du Control Panel).

TYPE DE BOÎTES AUX LETTRES	EXPLICATION
Boîte aux lettres LDAP	Les données utilisateur de cette boîte aux lettres sont synchronisées dans le Control Panel avec un service d'annuaire via LDAP. Pour de plus amples informations sur la synchronisation des boîtes aux lettres via LDAP, voir Synchroniser les utilisateurs et groupes avec LDAP.

Création automatique de boites aux lettres

Au lieu d'ajouter manuellement des boîtes aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220) ou de les importer dans le Control Panel (voir Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223), les boîtes aux lettres peuvent être créées automatiquement dans le Control Panel de deux façons différentes :

- Les boîtes aux lettres Microsoft 365 (voir Types de boîtes aux lettres à la page 218) sont synchronisés avec service d'annuaire.
- Les boîtes aux lettres sont automatiquement reconnues et créées à partir des adresses des destinataires des courriels acceptés par le serveur de courriels du client. Une boîte aux lettres

est alors enregistrée dans le Control Panel pour chaque adresse de destinataire. La création automatique de boîtes aux lettres est activée par défaut.

PRUDENCE :

Pour éviter la création de boîtes aux lettres inutiles et les surcouts que cela implique, il est nécessaire de configurer une vérification d'utilisateurs qui n'autorise que les courriels destinés à des boîtes aux lettres valides (voir Procéder à la configuration de l' environnement principal à la page 457).

PRUDENCE :

Le mécanisme de création automatique de boîtes aux lettres est incapable de faire à lui seul la différence entre les alias des boîtes aux lettres et les boites aux lettres principales lorsque la vérification des utilisateurs est active tant que les données de boîtes aux lettres ne sont pas synchronisées via un service de répertoire. Pour éviter la création automatique de boîtes aux lettres inutiles en raison de courriels entrants sur des adresses d'alias valides, les adresses d'alias doivent, en l'absence de synchronisation, être saisies manuellement dans le Control Panel (voir Ajouter une adresse alias à la page 243).

Ajouter une boîte aux lettres

Nos services peuvent être appliqués aux boîtes aux lettres enregistrées dans le Control Panel sous votre domaine. Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez ajouter des boîtes aux lettres à votre domaine dans le Control Panel.

IMPORTANT :

Les clients qui ont configuré la synchronisation des boîtes aux lettres avec un service d'annuaire via LDAP dans leur environnement primairel peuvent ajouter manuellement de nouvelles boîtes aux lettres uniquement s'ils ont créé un environnement secondaire (voir Créer un environnement secondaire à la page 116). Les boîtes aux lettres ajoutées manuellement ne sont pas synchronisées via ou LDAP.

IMPORTANT :

Si une nouvelle boîte aux lettres est ajoutée et que celle-ci a le même nom qu'une boîte aux lettres préalablement supprimée (voir Supprimer une boîte aux lettres à la page 262), cette boîte aux lettres du même nom dans le Control Panel n'aura aucun lien avec la boîte aux lettres préalablement supprimée.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine auquel vous souhaitez ajouter une nouvelle boîte aux lettres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur **Ajouter boîte aux lettres**.

Un formulaire s'ouvre.

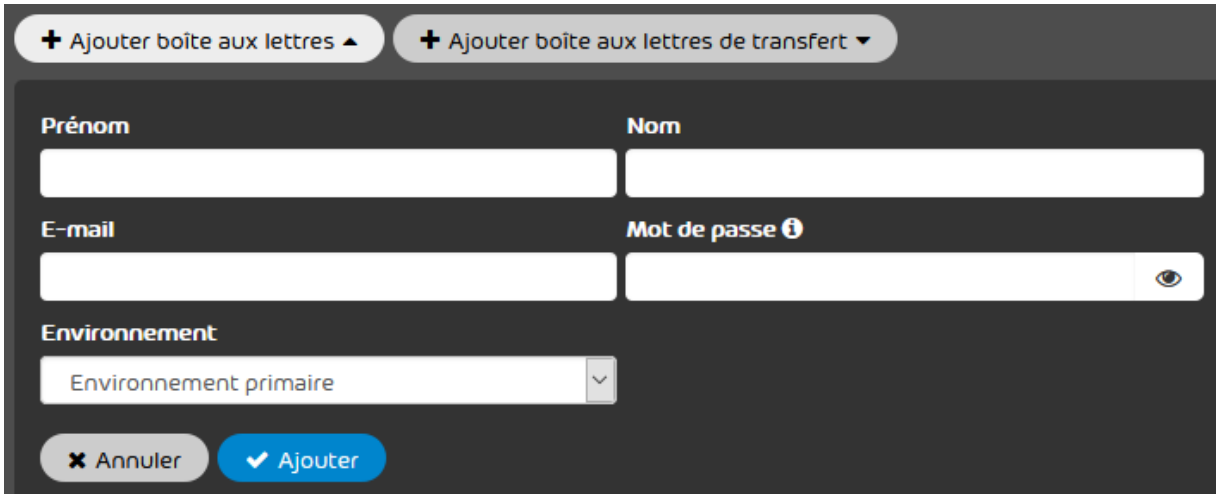


Illustration 170 : Formulaire

5. Dans le champ **Prénom**, saisissez le prénom du propriétaire de la boîte aux lettres.
6. Dans le champ **Nom**, saisissez le nom de famille du propriétaire de la boîte aux lettres.

7. Dans le champ **Courriel**, saisissez l'adresse courriel de la boîte aux lettres.

> **REMARQUE :**
>
> Les caractères spéciaux suivants sont pris en charge dans les adresse courriel :
>
> - Losange #
> - Et signe &
> - Apostrophe '
> - Signe plus +
> - Barre oblique /
> - Signe égal =
> - Point d'interrogation ?
> - Accent grave `
> - Barre verticale |
>
> Les caractères spéciaux suivants ne sont pas pris en charge :
>
> - Astérisque *
> - Point d'exclamation !
> - Signe de pourcentage %
> - Espace
> - Virgule ,

8. > **IMPORTANT :**
>
> Le mot de passe doit être conforme à la politique de mot de passe. La politique de mot de passe s'affiche dès que le curseur de la souris passe sur le symbole au-dessus du champ.

Dans le champ **Mot de passe**, saisissez un mot de passe permettant au propriétaire de la boîte aux lettres de s'identifier en tant qu'utilisateur dans le Control Panel.

9. Dans le menu déroulant sous **Environnement**, sélectionnez l'environnement vers lequel le trafic de courriels entrants de la boîte aux lettres doit être dirigé.

> **REMARQUE :**
>
> L'environnement définit vers quel serveur de destination est dirigé le trafic des courriels entrants de la boîte aux lettres. Le trafic de courriels entrants peut être dirigé vers l'environnement primaire (voir Procéder à la configuration de l'environnement principal à la page 457) ou vers un environnement secondaire (voir Environnements secondaires à la page 113) du domaine. les clients qui ont configuré la synchronisation des boîtes aux lettres avec un service d'annuaire dans leur environnement principal peuvent sélectionner uniquement des environnements secondaires.

10. Cliquez sur **Ajouter**.

La boîte aux lettres est créée et ajoutée à la liste de boîtes aux lettres.

Une boîte aux lettres est ajoutée au domaine dans le Control Panel.

Importer des boîtes aux lettres à partir d'un fichier CSV

Au lieu de saisir les boîtes aux lettres manuellement dans le Control Panel, vous pouvez importer des boîtes aux lettres à partir d'un fichier CSV dans le module **Paramètres client** > **Boîtes aux lettres**. Vous pouvez importer des boîtes aux lettres dans un premier temps, avant que d'autres boîtes aux lettres n'aient été créées dans le Control Panel, ou vous pouvez les importer ultérieurement. Vous pouvez mettre à jour ou supprimer des entrées qui existent déjà dans le Control Panel. Lors de l'importation, les boîtes aux lettres principales sont importées avec leurs adresses alias et les environnements ainsi que d'autres données dans le Control Panel.

> **REMARQUE :**
>
> Pour de plus amples informations sur les données qui peuvent être importées, voir Fichiers CSV pour importer des boîtes aux lettres à la page 227.

REMARQUE :

Les boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218) ne peuvent pas être importées depuis un fichier CSV.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez importer les boîtes aux lettres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur **Importer au format CSV**.

Un menu s'ouvre.

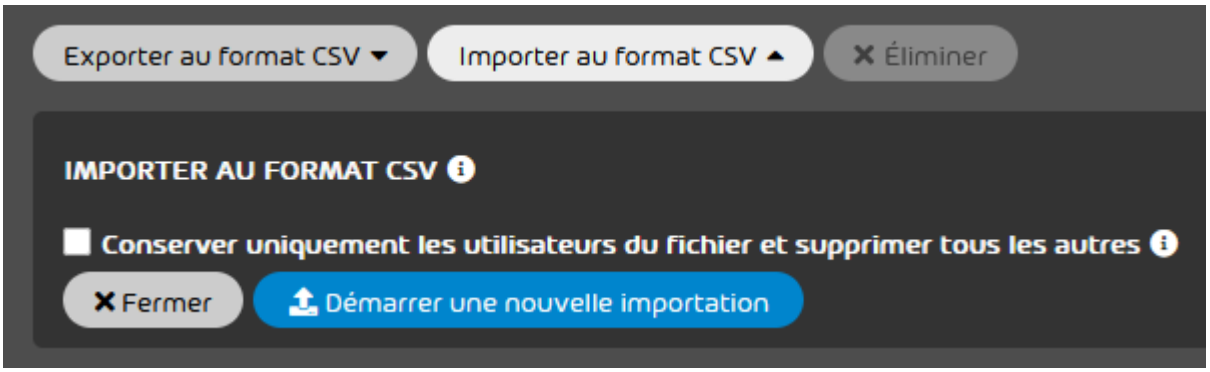


Illustration 171 : Menu pour l' importation CSV de boîtes aux lettres

5. **PRUDENCE :**

   Lors d'une importation CSV avec l'option **Conserver uniquement les utilisateurs du fichier et supprimer tous les autres**, les boîtes aux lettres existantes sont supprimées dans le Control Panel.

   Pour éviter de perdre des données, exportez les boîtes aux lettres existantes avant l'importation. Bien que le format du fichier exporté ne soit pas valide pour l'importation, le fichier peut toutefois être utile à des fins d'information.

   Facultatif : Pour supprimer toutes les boîtes aux lettres existantes dans le système avant d'importer de nouvelles boîtes aux lettres, cochez la case **Conserver uniquement les utilisateurs du fichier et supprimer tous les autres**.

6. Cliquez sur **Charger fichier**.

   REMARQUE :

   S'il ne s'agit pas de la première importation, le texte sur le bouton sera **Démarrer une nouvelle importation**.

   Une fenêtre de sélection des fichiers s'ouvre.

7. **IMPORTANT :**

   Pour s'assurer qu'un fichier CSV externe peut être importé dans le Control Panel sans erreur, des règles doivent être observées concernant le format du fichier, sa structure de contenu et une syntaxe valide (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227). La taille du fichier CSV ne doit pas dépasser 100 Mo.

   Sélectionnez le fichier CSV désiré.

   Le Control Panel lit le fichier CSV. Si le fichier est bien formé, le Control Panel analyse les données de boîte aux lettres qu'il contient et essaie de les importer. Les boîtes aux lettres qui n'existent pas encore sont créées dans le Control Panel et les boîtes aux lettres existantes sont mises à jour. Ensuite, un récapitulatif des boîtes aux lettres ajoutées

et mises à jour ainsi que, le cas échéant, les entrées CSV avec le type d'erreur indiqué apparaissent.

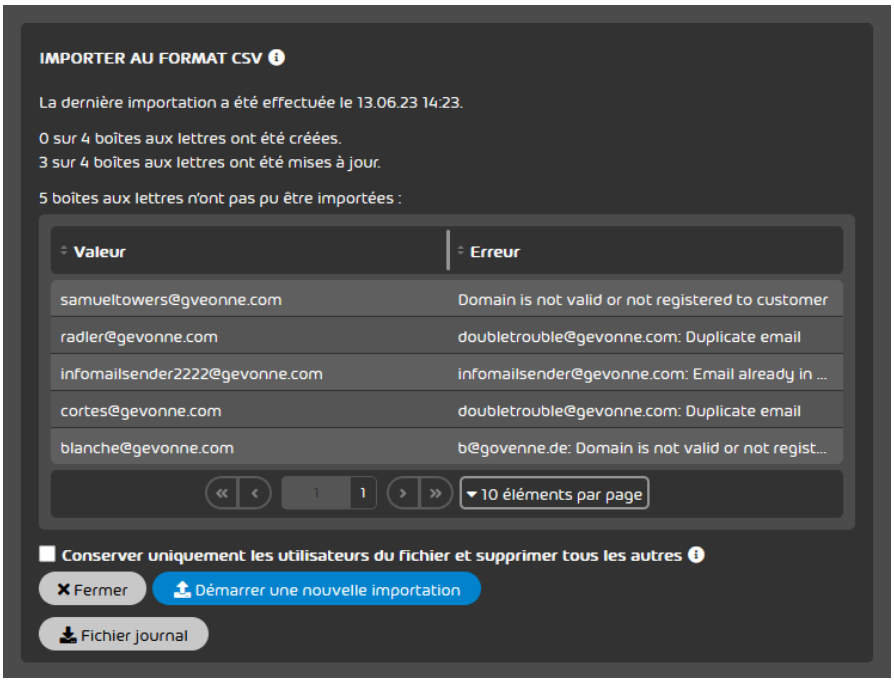


Illustration 172 : Résultat de l'importation

REMARQUE :

En fonction de la taille du fichier, l'importation peut prendre un certain temps. Pendant l'importation, une barre de progression apparaît dans le module **Paramètres client** > **Boîtes aux lettres**. Pour les fichiers qui contiennent plus de 1000#entrées, la progression est affichées par étapes de 1000#entrées. L'administrateur peut quitter le module sans que cela n'interrompe l'importation et la reprendre à un moment ultérieur.

REMARQUE :

Pour de plus amples informations sur les erreurs possibles, voir Erreur lors de l'importation de boîtes aux lettres à la page 232.

8. Facultatif : Pour obtenir de plus amples informations sur le résultat de l'importation, cliquez sur **Fichier journal**.

   UN fichier de protocole avec le nom **task.log** est téléchargé. Le fichier contient une liste de boîtes aux lettres avec une indication sur le temps de traitement, le résultat de l'importation et l'erreur survenue.

9. Cliquez sur **Fermer**.

   Le menu se ferme.

Les boîtes aux lettres sont importées depuis un fichier CSV et ajoutées au domaine sélectionné dans le Control Panel.

> **REMARQUE :**
>
> Les résultats de la dernière importation restent dans le système. Les administrateurs peuvent consulter les résultats dans le module **Paramètres client** > **Boîtes aux lettres** dans **Importer au format CSV**.

Fichiers CSV pour importer des boîtes aux lettres

Pour garantir qu'un fichier CSV externe contenant des données de boîtes aux lettres puisse être importé dans le Control Panel sans erreur (voir Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223), des règles doivent être observées pour l'extension des fichiers et la structure du contenu.

Conditions de base pour les fichiers CSV

- L'extension du fichier à importer est **.csv**. Les autres extensions de fichier telles que .txt ou .docx ne seront pas acceptées.
- Le fichier CSV doit être codé UTF-8.
- La taille du fichier CSV ne doit pas dépasser 100 Mo.

Colonnes

Le fichier CSV contient 19 colonnes séparées les unes des autres par un point-virgule. Ces colonnes sont destinées aux informations suivantes :

1. Adresse courriel primaire de la boîte aux lettres.

   > **IMPORTANT :**
   >
   > La colonne ne doit pas contenir des lignes vides.

2. Adresse alias de la boîte aux lettres
3. Environnement de la boîte aux lettres. L'environnement définit vers quel serveur de destination est dirigé le trafic des courriels entrants d'une boîte aux lettres (voir Environnements secondaires à la page 113).

   > **IMPORTANT :**
   >
   > La colonne ne doit pas contenir des lignes vides.

4. Prénom de l'utilisateur
5. Nom de famille de l'utilisateur
6. Nom de l'utilisateur affiché dans le Control Panel
7. Pays ou région où se trouve l'organisation de l'utilisateur
8. Land ou canton où se trouve l'organisation de l'utilisateur
9. Code postal de l'organisation de l'utilisateur
10. Lieu où se trouve l'organisation de l'utilisateur
11. Rue ou numéro de maison où se trouve l'organisation de l'utilisateur
12. Service dans lequel travaille l'utilisateur

13. Bureau où travaille l'utilisateur
14. Numéro de téléphone professionnel de l'utilisateur
15. Numéro de téléphone mobile de l'utilisateur
16. Numéro de fax de l'utilisateur
17.
18.
19. Les groupes auxquels la boîte aux lettres appartient (voir Groupes à la page 268)

> **IMPORTANT :**
>
> La première colonne (adresse courriel primaire) et la troisième colonne (environnement) doivent contenir des données. Toutes les autres colonnes sont optionnelles et peuvent donc être vides. Chaque ligne doit cependant contenir 18 points-virgules comme caractères de séparation.

> **REMARQUE :**

Lignes

- Les lignes du fichier CSV s'achèvent sans signe de ponctuation.
- La première ligne contient les noms des colonnes. Les noms des colonnes peuvent être choisis librement et n'ont aucune influence sur le succès de l'importation. Pour une meilleur compréhension, il est toutefois recommandé d'utiliser des noms de colonnes descriptifs.

Adresses de boîtes aux lettres

- Les adresses des boîtes aux lettres sont bien formées (selon le modèle **partielocale@nomhote.domaine-principal**).

> **IMPORTANT :**
>
> Les adresses mal formées ne sont pas prises en compte lors de l'importation.

- Les adresses des boîtes aux lettres appartiennent aux domaines qui ont été enregistrés pour le client dans le Control Panel.

> **IMPORTANT :**
>
> Les adresses des boîtes aux lettres d'autres domaines ne sont pas importées dans le Control Panel.

Adresses alias

- Les adresses alias (dans la deuxième colonne) ne doivent être indiquées qu'en combinaison avec l'adresse courriel primaire de la boîte aux lettres (dans la première colonne). La première colonne ne doit pas être vide.
- Si une cellule de la deuxième colonne contient plusieurs adresses alias, les adresses distinctes sont séparées par des virgules.

Boîte aux lettres principale sans adresse alias et avec environnement primaire (sans autres indications) :

boiteprincipale@seule.fr;;primaire;;;;;;;;;;;;;;;;

Boîte aux lettres principale avec une adresse alias et un environnement primaire (sans autres indications) :

boiteprincipale@exemple.fr;alias@exemple.fr;primaire;;;;;;;;;;;;;;;;

Boîte aux lettres principale avec plusieurs adresses alias et un environnement primaire (sans autres indications) :

boiteprincipale@exemple.fr;alias1@exemple.fr,alias2@exemple.fr;primaire;;;;;;;;;;;;;;;;

Environnements

- Les environnements devant être attribués aux boîtes aux lettres à importer dans le Control Panel doivent être indiqués dans la troisième colonne de chaque ligne.
- Pour l'environnement primaire, le nom **primary** est utilisé. Pour les environnements secondaires, le nom sous lequel s'affiche l'environnement secondaire dans le Control Panel est utilisé. La casse n'a aucune importance pour les noms des environnements.

> **IMPORTANT :**
>
> Les entrées avec environnements secondaires peuvent être importées d'un fichier CSV uniquement si les environnements secondaires ont été créés au préalable dans le Control Panel (voir Créer un environnement secondaire à la page 116).

Boîte aux lettres principale avec une adresse alias et un environnement primaire (sans autres indications) :

boiteprincipale@exemple.fr;alias@exemple.fr;primaire;;;;;;;;;;;;;;;;

Boîte aux lettres principale avec une adresse alias et un environnement secondaire (sans autres indications) :

boîteauxlettresprincipale@exemple.fr;alias@exemple.fr;environnement2;;;;;;;;;;;;;;;;

Groupes

- Les groupes auxquels les boîtes aux lettres à importer appartiennent sont indiqués dans la colonne 19.
- Si une cellule de la colonne 19 contient plusieurs groupes, les différents groupes seront séparés l'un de l'autre par des virgules.

Entrées en double

- Les entrées en double n'entraînent pas un échec de l'importation pendant le traitement du fichier CSV, mais doivent toutefois être évités.
- Le fichier ne doit pas contenir de lignes qui ont le même contenu dans la colonne de gauche mais un contenu différent dans l'autre colonne.

> **IMPORTANT :**
>
> Les lignes avec la même boîte aux lettres principale ne sont pas importées si le fichier CSV contient une autre ligne avec la même boîte aux lettres principale mais des adresses alias différentes ou un autre environnement.

Les lignes non autorisées avec la même boîte aux lettres, des adresses alias différentes et un environnement principal (sans autres indications) :

boiteprincipale@exemple.fr;alias1@exemple.fr,alias2@exemple.fr;primaire;;;;;;;;;;;;;;;;
boiteprincipale@exemple.fr;alias3@exemple.fr;primaire;;;;;;;;;;;;;;;;

Erreur lors de l'importation de boîtes aux lettres

Lors de l'importation de boîtes aux lettres (voir Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223), le Control Panel effectue différents contrôles l'un à la suite de l'autre, qui peuvent renvoyer des erreurs différentes. Le fichier CSV est d'abord validé et les données de boîte aux lettres qu'il contient sont ensuite vérifiées et traitées.

Erreur lors de la validation de fichiers CSV

Le fichier CSV est validé dès que l'utilisateur l'a sélectionné pour importer des boîtes aux lettres. Il est alors notamment vérifié si le fichier CSV est bien formé. Les erreurs possibles sont :

- **Une erreur est survenue lors du chargement de l'état de l'importation en cours.**
- **Une erreur est survenue lors de la validation du fichier.**
- **Une erreur est survenue lors du traitement du fichier.**

- **Une ligne dans le fichier est trop longue.** : Le fichier contient une ligne dont la taille est supérieure à 1 Mo (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227).
- **Le codage du fichier doit être {{encodingType}}.** : Le fichier n'est pas codé avec UTF-8 (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227).
- **Le service de chargement est actuellement inaccessible.**
- **Le fichier a un nombre de colonnes incorrect.** : Le fichier ne contient pas 19 colonnes dans chaque ligne (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227).

Erreurs lors de la traitement de boîtes aux lettres

Après que le fichier CSV a été validé, les données de boîte aux lettres qu'il contient sont vérifiées pour s'assurer qu'elles sont bien formées et qu'elles ne contiennent pas de doublons. Il est également vérifié si les environnements (voir Configuration d'environnement principal à la page 456 et Environnements secondaires à la page 113) et les domaines (voir Domaines à la page 285) existent dans le Control Panel et sont attribués au client, et si les boîtes aux lettres appartiennent à un environnement dont les boîtes aux lettres sont synchronisées avec un service d'annuaire.

1. **Data is invalid** : Certaines données de boîte aux lettres ne sont pas bien formées sans explication.
2. **Email is not valid** : L'adresse courriel entrée n'est pas bien formée.
3. **Domain is not valid or not registered to customer** : Le domaine de l'adresse courriel entrée (adresse primaire ou adresse alias) n'est pas entrée dans le Control Panel pour le client (voir Ajouter un domaine d'alias à la page 286).
4. **Email already in use** : Une boîte aux lettres avec la même adresse courriel existe déjà dans le Control Panel.
5. **Unknown error** : Une erreur inconnue est survenue.
6. **User creation failed** : L'utilisateur pour la boîte aux lettres n'a pas pu être créé dans le Control Panel.

7. **Failed to import** : L'entrée n'a pas pu être importée pour d'autres raisons.
8. **Synchronized mailboxes needs to be changed in the source system** : L'entrée concernée fait référence à une boîte aux lettres synchronisée avec un service d'annuaire dans le Control Panel.
9. **Unable to assign the primary environment to the manual mailbox** : Les boîtes aux lettres de l'environnement primaire (voir Configuration d'environnement principal à la page 456) sont synchronisées avec un service d'annuaire. Il n'est donc pas possible d'attribuer une boîte aux lettres créée manuellement à cet environnement.
10. **The primary email appeared on two users in the request at the same time** : Le fichier CSV contient deux entrées avec la même adresse courriel dans la première colonne (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227).
11. **Duplicate email** : Une adresse courriel est utilisée dans plus d'une entrée, qu'il s'agisse d'une adresse courriel primaire ou d'une adresse alias.

Exporter des boîtes aux lettres sous un fichier CSV

Vous avez ajouté des boîtes aux lettres dans le Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223).

Pour éviter toute perte des données des boîtes aux lettres de votre domaine, vous pouvez exporter les données des boîtes aux lettres sous forme de fichier CSV. Lors de l'exportation, les données de toutes les boîtes aux lettres disponibles dans le Control Panel sous le domaine sont exportées.

IMPORTANT :

Les données d'exportation ne sont pas destinées à l'importation dans le Control Panel (voir Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223), car elles ont un format différent (voir Fichiers CSV pour importer des boîtes aux lettres à la page 227).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez exporter les boîtes aux lettres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur **Exporter au format CSV**.

Un formulaire apparaît.

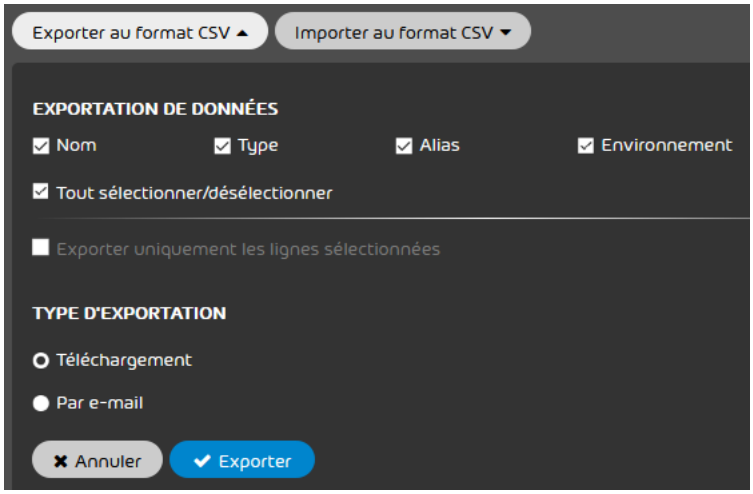


Illustration 173 : Formulaire pour l' exportation CSV

5. Sous **Exportation de données**, cochez la case des données que vous souhaitez exporter.
   - **Nom** : les adresses des boîtes aux lettres principales sont exportées.
   - **Type** : les types de boîtes aux lettres principales sont exportées (voir Boîtes aux lettres à la page 213).
   - **Alias** : Si des adresses alias sont attribuées à des boîtes aux lettres principales, les adresses alias sont exportées.
   - **Environnement** : les environnements des boîtes aux lettres sont exportés (voir Ajouter une boîte aux lettres à la page 220).
   - **Sélectionner/désélectionner tout** : toutes les cases décrites au préalable sont sélectionnées ou désélectionnées.

6. Facultatif : Si vous souhaitez exporter uniquement les boîtes aux lettres sélectionnées, procédez comme suit :

   a) Cliquez sur en haut du module.

Une colonne avec des cases à cocher s'affiche dans le tableau.

   b) Sélectionnez les lignes à partir desquelles vous souhaitez exporter des données.

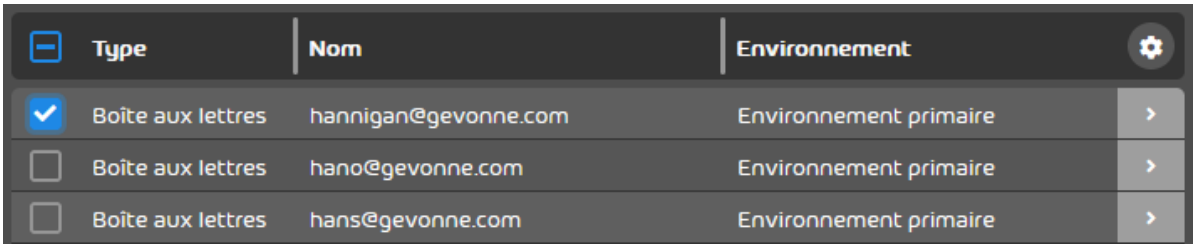


Illustration 174 : Sélectionner des lignes

La case **Exporter uniquement les lignes sélectionnées** est déverrouillée dans le formulaire.

   c) Cochez la case **Exporter uniquement les lignes sélectionnées**.

Illustration 175 : Exporter les lignes sélectionnées

7. Sous **Type d'exportation**, indiquez si le fichier CSV doit être mis à disposition en téléchargement ou envoyé par courriel.
   - **Téléchargement** : le fichier CSV est mis à disposition dans les téléchargements.
   - **Par courriel** : le fichier CSV est envoyé par courriel.

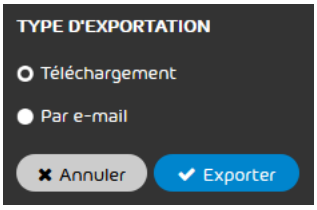


Illustration 176 : Sélectionner le type d'exportation

Si l'option **Par courriel** a été sélectionnée, un champ supplémentaire s'affiche.

8. Facultatif : Si vous avez sélectionné l'option **Par courriel**, saisissez l'adresse courriel à laquelle le fichier CSV doit être envoyé dans le champ.

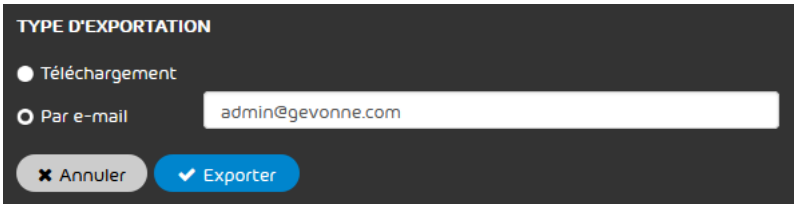


Illustration 177 : Saisir une adresse courriel

9. Cliquez sur **Exporter**.

Le fichier est mis à disposition dans les téléchargements ou envoyé par courriel.

Les boîtes aux lettres ont été exportées sous la forme d'un fichier CSV.

Ajouter boîte aux lettres de redirection

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez configurer des boîtes aux lettres de redirection pour les boîtes aux lettres existantes. Les boîtes aux lettres de redirection peuvent rediriger le trafic de courriels vers une à 100 boîtes aux lettres internes ou externes.

IMPORTANT :

La taille maximale autorisée pour les courriels transférés via des boîtes aux lettres de redirection est limitée et dépend du nombre de destinataires de la redirection. Le tableau suivant précise la taille autorisée des courriels transférés en fonction du nombre de destinataires.

NOMBRE DE DESTINATAIRES	TAILLE MAXIMALE AUTORISÉE POUR LES COURRIELS (MO)
1	100
2-9	50
10-24	25
25-49	15
50-100	10

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine auquel vous souhaitez ajouter une boîte aux lettres de redirection.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur **Ajouter boîte aux lettres de transfert**.

Un menu déroulant s'ouvre.

5. Dans **Adresse e-mail**, saisissez la boîte aux lettres pour laquelle une redirection doit être configurée. (1)
6. Pour ajouter une boîte aux lettres de redirection,
   - sélectionnez une boîte aux lettres enregistrée dans la liste (2a) ou
   - saisissez une adresse courriel valide dans le champ **Boîte aux lettres externe** (2b) et confirmez avec **Ajouter**

> **REMARQUE :**
>
> Répétez cette étape pour ajouter d'autres boîtes aux lettres de redirection.

Les boîtes aux lettres apparaissent dans la liste **Transmet à**.

7. Cliquez sur **Ajouter** (3) pour configurer la redirection.

Une boîte aux lettres de redirection a été ajoutée.

Ajouter une boîte aux lettres à un groupe

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).
Vous avez créé un groupe (voir Créer un groupe à la page 270).

Au lieu d'ajouter des boîtes aux lettres à un groupe (voir Gérer les membres à la page 277) dans le module **Groupes**, vous pouvez ajouter une boîte aux lettres à un groupe (voir Groupes à la page 268) dans le module **Boîtes aux lettres**.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine auquel vous souhaitez ajouter une boîte aux lettres au groupe.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche du menu à côté de la boîte aux lettres que vous souhaitez ajouter à un groupe.

Un menu s'ouvre.

Illustration 178 : Actions pour les boîtes aux lettres

5. Cliquez sur **Groupes**.

Un menu de gestion des groupes s'ouvrent. Tous les groupes auxquels la boîte aux lettres appartient apparaissent ici.

Illustration 179 : Menu des groupes

6. Dans le champ de saisie, saisissez le nom du groupe auquel vous souhaitez ajouter la boîte aux lettres.

7. Cliquez sur **Ajouter**.

La boîte aux lettres est ajoutée au groupe. Le groupe est affiché de la liste des groupes.

Une boîte aux lettres est ajoutée à un groupe.

Vous pouvez ensuite supprimer la boîte aux lettres du groupe (voir Supprimer une boîte aux lettres d'un groupe à la page 241).

Supprimer une boîte aux lettres d'un groupe

Vous avez ajouté une boîte aux lettres à un groupe (voir Ajouter une boîte aux lettres à un groupe à la page 239).

Au lieu de supprimer des boîtes aux lettres d'un groupe dans le module **Groupes** (voir Gérer les membres à la page 277), vous pouvez supprimer une boîte aux lettres d'un groupe dans le module **Boîtes aux lettres** (voir Groupes à la page 268).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine auquel vous souhaitez supprimer une nouvelle boîte aux lettres du groupe.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche du menu à côté de la boîte aux lettres que vous souhaitez supprimer d'un groupe.

Un menu s'ouvre.

Illustration 180 : Actions pour les boîtes aux lettres

5. Cliquez sur **Groupes**.

Un menu de gestion des groupes s'ouvrent. Tous les groupes auxquels la boîte aux lettres appartient apparaissent ici.

Illustration 181 : Menu des groupes

6. Cliquez sur le symbole de croix à côté du groupe dont vous souhaitez supprimer la boîte aux lettres.

La boîte aux lettres est supprimée du groupe. Le groupe est supprimé de la liste des groupes.

Une boîte aux lettres a été supprimée d'un groupe.

Activer ou désactiver une boîte aux lettres

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).

Seuls les utilisateurs dont les boîtes aux lettres sont activées dans le Control Panel peuvent se connecter au Control Panel. Nos services sont appliqués et facturés de la même manière aux boîtes aux lettres activées et désactivées. Vous pouvez activer et désactiver les boîtes aux lettres dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.

4. Cliquez sur la flèche du menu à côté de la boîte aux lettres que vous souhaitez activer ou désactiver.

Illustration 182 : Ouvrir le menu

- Un menu s'ouvre.

5. Cliquez sur le bouton **Actif** ou **Inactif**.

- Un menu déroulant s'ouvre.

6. Cliquez sur **Activer** ou **Désactiver**.

- La boîte aux lettres est activée ou désactivée. Selon l'état d'activation, le symbole sera blanc (activé) ou rouge (désactivé).

Une boîte aux lettres est activée ou désactivée.

Ajouter une adresse alias

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez ajouter des adresses alias à une boîte aux lettres principale. Une adresse alias est attribuée à une boîte aux lettres principale. Pour le propriétaire d'une boîte aux lettres, les courriels des adresses alias s'affichent à côté des courriels de la boîte aux lettres principale dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59). Vous pouvez ajouter plusieurs adresses alias à une boîte aux lettres principale. Aucun frais n'est facturé pour les adresses alias.

REMARQUE :

Aucune adresse alias ne peut être ajoutée aux boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218).

ATTENTION :

Si les données des boîtes aux lettres d'un client ne sont pas synchronisées via un service de répertoire, le client doit ajouter manuellement toutes les adresses alias du domaine au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223). Autrement, lors de la création automatique de boîtes aux lettres (voir Création automatique de boites aux lettres à la page 219), les adresses alias ne seraient pas reconnues comme des adresses alias de boîtes aux lettres principales existantes, mais comme nouvelles boîtes aux lettres principales. Des boîtes aux lettres principales gratuites seraient alors créées dans le Control Panel pour les adresses alias (voir Boîtes aux lettres à la page 213).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine de la boîte aux lettres principale à laquelle vous souhaitez ajouter une adresse alias.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche du menu à côté de la boîte aux lettres à laquelle vous souhaitez ajouter une adresse alias.

Illustration 183 : Ouvrir le menu

Un menu s'ouvre.

5. Cliquez sur **Alias**.

Un menu s'ouvre.

6. Saisissez sous **Alias** l'alias désiré suivi du domaine et cliquez sur **Ajouter**.

Illustration 184 : Saisir une adresse alias

L'adresse alias est ajoutée.

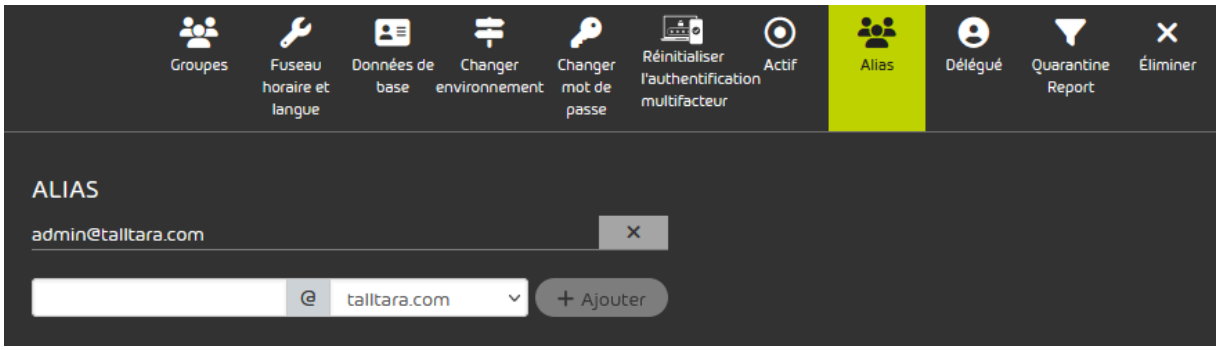


Illustration 185 : Adresse alias ajoutée

Une adresse alias est ajoutée à une boîte aux lettres principale.

Saisir une délégation

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez saisir une délégation pour une boîte aux lettres principale existante. Dans le module **Email Live Tracking** (voir Email Live Tracking

à la page 59), les remplaçants ont accès aux courriels de la boîte aux lettres pour laquelle ils sont enregistrés en tant que remplaçant et peuvent effectuer des actions des courriels pour ces courriels.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la zone de l'espace, sélectionnez le domaine de la boîte aux lettres pour laquelle vous souhaitez saisir une délégation.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche de menu de la boîte aux lettres désirée.

5. Cliquez sur **Délégué**.

➔ Un menu déroulant s'ouvre.

6. Cochez la case **Activer accès de délégué**.

➔ Une liste des utilisateurs enregistrés apparaît.

7. Sélectionnez une délégation dans la liste et cliquez sur **Ajouter**.

➔ La délégation est ajoutée à la boîte aux lettres. Pour des raisons de sécurité, l'utilisateur dont la boîte aux lettres a été attribuée à la délégation est averti par courriel de l'attribution de la délégation.

✓ Une délégation a été saisie pour une boîte aux lettres.

Importer des destinataires de boîtes aux lettres de redirection à partir d’ un fichier CSV

Au lieu de saisir manuellement les destinataires des boîtes aux lettres de redirection, vous pouvez les importer à l'aide d'une liste CSV dans le module **Paramètres client** > **Boîtes aux lettres**. Ceci peut avoir lieu à la fois dans un premier temps, si aucune donnée n'a encore été saisie, et en complément en cours d'exploitation.

REMARQUE :

Aucune boîte aux lettres de redirection ne peut être attribuée aux boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218). Par conséquent, il n'est pas possible d'importer des destinataires de boîtes aux lettres de redirection à partir d'un fichier CSV pour ces boîtes aux lettres.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur **Ajouter**.

Un nouveau formulaire apparaît.

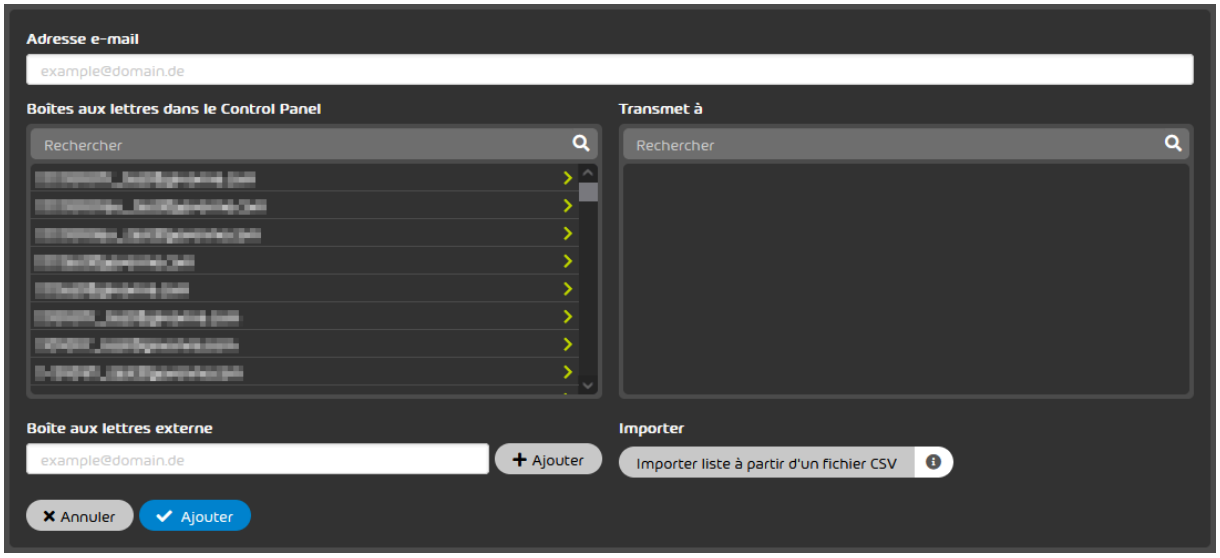


Illustration 186 : Importer des destinataires pour une boîte aux lettres de redirection à partir d' un fichier CSV

5. Saisissez sous **Adresse e-mail** l'adresse courriel de la boîte aux lettres de redirection.
6. Cliquez sur **Importer liste à partir d'un fichier CSV**.

Une fenêtre de sélection des fichiers s'ouvre.

7. Sélectionnez le fichier CSV désiré.

> **IMPORTANT :**
>
> Pour s'assurer qu'un fichier CSV externe peut être importé dans le Control Panel sans erreur, des règles spéciales doivent être observées concernant le format du fichier, sa structure de contenu et une syntaxe valide (voir Fichiers CSV pour l' importation de destinataires pour les boîtes aux lettres de redirection à la page 249).

8. Cliquez sur **Importer liste à partir d'un fichier CSV**.

Les destinataires sont importés à partir du fichier CSV et affichés dans la section **Transmet à**.

REMARQUE :

Les règles suivantes s'appliquent lors de l'importation de destinataires pour les boîtes aux lettres de redirection#:

- Les destinataires apparaissant déjà dans **Transmet à** ne sont pas supprimés.
- Seules des entrées du fichier CSV qui ne sont pas déjà affichées sous **Transmet à** sont importées.
- Les entrées qui sont en double dans le fichier CSV ne sont importées qu'une seule fois.
- Les entrées de la liste mal formées sont ignorées et n'entraînent pas la fin de l'opération. Toutefois, après l'importation, un message d'erreur s'affiche s'il existe des entrées non valables.
- Si un fichier CSV ne contient pas d'adresse valide déjà présente dans la section **Transmet à**, un message d'erreur apparaît et aucune adresse n'est importée.

9. Cliquez sur **Ajouter**.

Des destinataires de boîtes aux lettres de redirection ont été importés à partir d'un fichier CSV.

Fichiers CSV pour l'importation de destinataires pour les boîtes aux lettres de redirection

Pour garantir qu'un fichier CSV externe contenant des destinataires de boîtes aux lettres de redirection puisse être importé dans le Control Panel sans erreur (voir Importer des destinataires de boîtes aux lettres de redirection à partir d'un fichier CSV à la page 247), des règles spéciales doivent être observées pour l'extension des fichiers et la structure du contenu.

Règles de structure d'un fichier CSV pour l'importation de destinataires pour les boîtes aux lettres de redirection

- L'extension du fichier à importer est toujours **.csv**. Les autres extensions de fichier telles que .txt ou .docx ne sont pas autorisées et ne seront pas acceptées.

- Le fichier CSV ne contient qu'une seule colonne dans laquelle les entrées individuelles sont saisies l'une après l'autre.
- La première ligne est toujours le nom de la colonne et peut être nommée individuellement.
- Les adresses des destinataires doivent être bien formées (selon le modèle « partie-locale@nom-d'hote.domaine-top-level »).

> **IMPORTANT :**
>
> Les adresses mal formées ne sont pas prises en compte lors de l'importation.

- Chaque ligne ne peut contenir qu'une seule adresse.
- Les doublons n'ont aucune influence sur le traitement du fichier, mais doivent être évités.

Définir le fuseau horaire et la langue d'une boîte aux lettres

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223).

Le module **Paramètres client** > **Boîtes aux lettres** (voir Boîtes aux lettres à la page 213) vous permet de définir pour une boîte aux lettres individuelle un fuseau horaire, une langue, un format de date et d'heure différents de ceux du domaine (voirle chapitre « Régler les valeurs par défaut pour le fuseau horaire et la langue » dans le manuel du Control Panel). Les paramètres s'appliquent à l'affichage dans le Control Panel et aux courriels automatiques du Control Panel. Les données de ce module sont synchronisées avec les données de l'utilisateur dans la section **Fuseau horaire et langue** sous **Paramètres utilisateur** (voir Modifier le fuseau horaire et la langue à la page 34).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine de la boîte aux lettres dont vous souhaitez modifier les paramètres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.

4. Cliquez sur la flèche de menu à côté de la boîte aux lettres dont vous souhaitez modifier les paramètres.

Illustration 187 : Ouvrir le menu

- Un menu s'ouvre.

Illustration 188 : Menu

5. Cliquez sur **Fuseau horaire et langue**.

- Un formulaire apparaît.

Illustration 189 : Fuseau horaire et langue

6. Dans le menu déroulant **Fuseau horaire**, sélectionnez un fuseau horaire.

> **REMARQUE :**
>
> Le fuseau horaire détermine le format des chiffres dans le Control Panel et dans les courriels automatiques du Control Panel.

7. Dans le menu déroulant **Langue**, sélectionnez une langue.

8. Dans le menu déroulant **Format de date**, sélectionnez un format de date.

> **REMARQUE :**
>
> Le format de date détermine l'ordre dans lequel les données disponibles d'une date sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

9. Dans le menu déroulant **Format d'heure**, sélectionnez un format d'heure.

> **REMARQUE :**
>
> Le format d'heure détermine l'ordre dans lequel les données disponibles d'une heure sont affichées. Si des informations ne sont pas disponibles pour toutes les données, les données manquantes ne seront pas affichées.

10. Cliquez sur **Enregistrer**.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Les modifications ne seront appliquées que lorsque l'utilisateur pour lequel les modifications ont été effectuées actualisera la page ou se connectera à nouveau au Control Panel.

Le fuseau horaire, la langue, le format de la date et de l'heure d'une boîte aux lettres ont été définis.

Éditer des données de base d' une boîte aux lettres

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).

Les données de base sont des informations sur le propriétaire d'une boîte aux lettres. Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez ajouter des données de base aux boîtes aux lettres.

REMARQUE :

Vous ne pouvez pas éditer les données de base dans le Control Panel pour les boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218). Si les données de base d'une boîte aux lettres sont stockées dans un service d'annuaire synchronisé par LDAP, ces données sont affichées dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le client désiré dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche du menu à côté de la boîte aux lettres dont vous souhaitez éditer les données de base.

Un menu s'ouvre.

Illustration 190 : Menu

5. Cliquez sur **Données de base**.

Un formulaire apparaît.

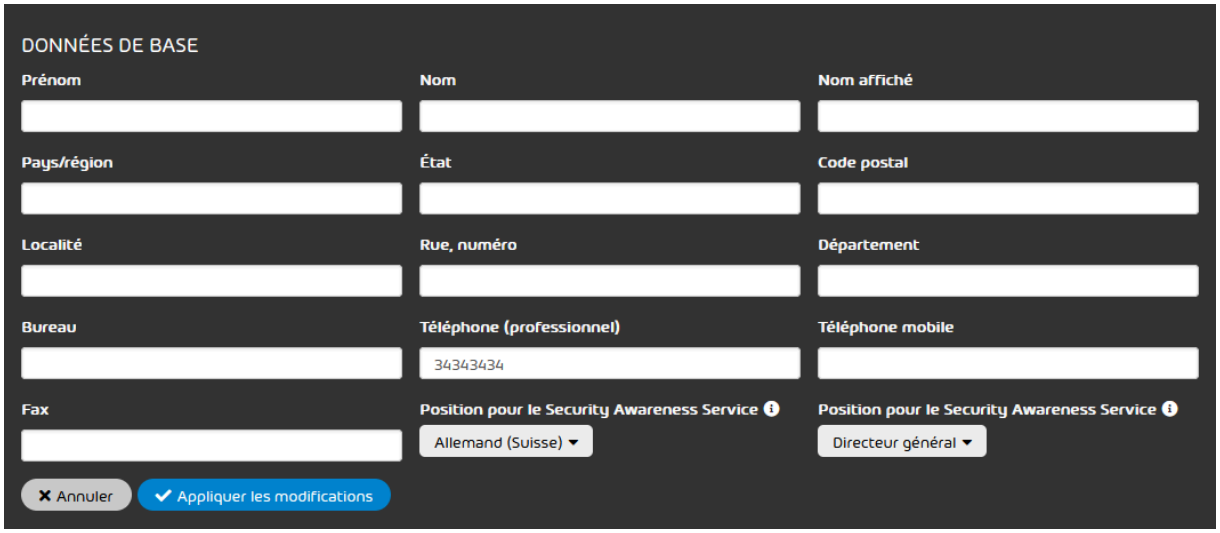


Illustration 191 : Données de base

6.

REMARQUE :

Tous les champs sont facultatifs.

REMARQUE :

Dans les champs **Téléphone (professionnel)**, **Téléphone mobile** et **Fax**, les numéros de téléphone ou de fax doivent être saisis dans le format suivant :

- Indicatif du pays : 00 ou + et indicatif de pays à deux chiffres. L'indicatif du pays peut également être mis entre parenthèses. Exemples d'indicatifs de pays corrects : **(0034)**, **(+34)**, **0049**, **+49**.
- Espace, point ou tiret pour séparer l'indicatif du pays de l'indicatif régional (facultatif).
- Indicatif régional ou de téléphonie mobile à cinq chiffres maximum.
- Espace, point ou tiret pour séparer l'indicatif régional ou de téléphonie mobile du numéro de téléphone (facultatif).
- Numéro de téléphone composé d'un nombre quelconque de chiffres.

Voici quelques exemples de numéros de téléphone ou de fax corrects :

- **(0034) 7432 1354913**
- **+49.157.1354913**
- **0049 157-1354913**

Dans le formulaire, saisissez les données de l'utilisateur qui possède la boîte aux lettres. Les champs ont les significations suivantes :

- **Prénom** : Prénom de l'utilisateur
- **Nom** : Nom de famille de l'utilisateur
- **Nom affiché** : Nom de l'utilisateur affiché dans le Control Panel
- **Pays/région** : Pays ou région où se trouve l'organisation de l'utilisateur
- **État** : Land ou canton où se trouve l'organisation de l'utilisateur
- **Code postal** : Code postal de l'organisation de l'utilisateur
- **Localité** : Lieu où se trouve l'organisation de l'utilisateur

- **Rue, numéro** : Rue ou numéro de maison où se trouve l'organisation de l'utilisateur
- **Département** : Service dans lequel travaille l'utilisateur
- **Bureau** : Bureau où travaille l'utilisateur
- **Téléphone (professionnel)** : Numéro de téléphone professionnel de l'utilisateur
- **Téléphone mobile** : Numéro de téléphone mobile de l'utilisateur
- **Fax** : Numéro de fax de l'utilisateur

7. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées.

Les données de base d'une boîte aux lettres ont été éditées.

Modifier le mot de passe d'urgence

Vos boîtes aux lettres sont synchronisées via LDAP obligé vos utilisateurs à créer un mot de passe d'urgence (voir Activer le mot de passe d'urgence).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez modifier le mot de passe d'urgence d'une boîte aux lettres.

REMARQUE :

Les mots de passe d'urgence ne peuvent être modifiés que pour les boîtes aux lettres LDAP (voir Types de boîtes aux lettres à la page 218).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.

4. Cliquez sur la flèche de menu à côté de la boîte aux lettres dont vous souhaitez modifier le mot de passe d'urgence.

5. Cliquez sur **Changer le mot de passe d'urgence**.

Un champ de saisie apparaît.

6. Saisissez votre mot de passe d'urgence dans le champ de saisie.

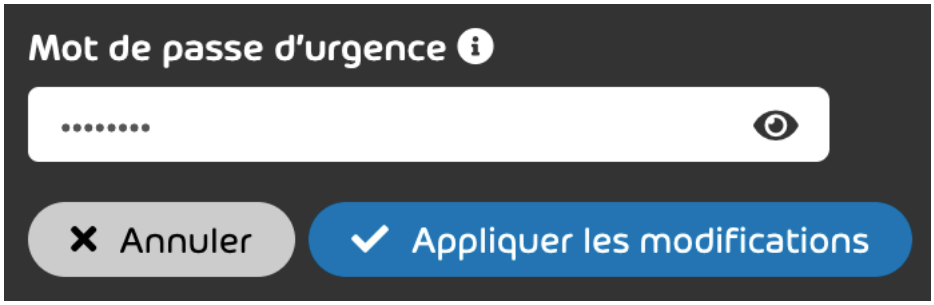


Illustration 192 : Changer le mot de passe d'urgence

7. Cliquez sur **Appliquer les modifications**.

Le mot de passe d'urgence est sauvegardé.

Le mot de passe d'urgence d'une boîte aux lettres a été modifié.

Modifier l'environnement

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223). Vous avez défini le serveur de destination vers lequel est dirigé le trafic de courriels entrants de la boîte aux lettres, comme environnement principal (voir Procéder à la configuration de

l'environnement principal à la page 457) ou environnement secondaire (voir Créer un environnement secondaire à la page 116).

L'environnement d'une boîte aux lettres définit vers quel serveur de destination est dirigé le trafic des courriels entrants de la boîte aux lettres. Par défaut, l'environnement principal (voir Configuration d'environnement principal à la page 456) est attribué aux boîtes aux lettres d'un domaine.
Si le trafic de courriels entrants de certaines boîtes aux lettres du domaine doit être dirigé vers un autre serveur de destination, vous pouvez attribuer un environnement secondaire à ces boîtes aux lettres, à la place de l'environnement principal (voir Environnements secondaires à la page 113).
Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez modifier les environnements des boîtes aux lettres de votre domaine. Vous ne pouvez attribuer aucun environnement dans le Control Panel aux boîtes aux lettres de redirection (voir Types de boîtes aux lettres à la page 218) et aux boîtes aux lettres synchronisées, car les boîtes aux lettres de redirection sont gérées sans environnement dans le Control Panel et, pour les boîtes aux lettres synchronisées, l'environnement du système d'origine s'applique.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la zone de sélection, sélectionnez le domaine de la boîte aux lettres dont vous souhaitez modifier l'environnement.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche du menu à côté de la boîte aux lettres dont vous souhaitez modifier l'environnement.

Illustration 193 : Ouvrir le menu

- Un menu s'ouvre.

5. Cliquez sur **Changer environnement**.

- Un formulaire apparaît.

6. Dans le menu déroulant sous **Environnement**, sélectionnez l'environnement vers lequel le trafic de courriels entrants de la boîte aux lettres doit être dirigé.

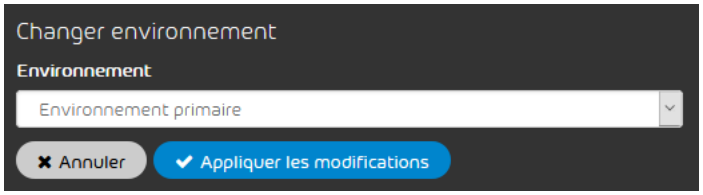


Illustration 194 : Sélectionner l'environnement

7. Cliquez sur **Appliquer les modifications**.

L'environnement d'une boîte aux lettres a été modifié.

Modifier le mot de passe

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez modifier le mot de passe pour une boîte aux lettres créée manuellement (voir Types de boîtes aux lettres à la page 218).

REMARQUE :

Les mots de passe des boîtes aux lettres LDAP ne peuvent être modifiés dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.

4. Cliquez sur la flèche du menu à côté de la boîte aux lettres dont vous souhaitez modifier le mot de passe.

Illustration 195 : Ouvrir le menu

- Un menu s'ouvre.

5. Cliquez sur **Changer mot de passe**.

- Un menu s'ouvre.

6.

> **IMPORTANT :**
>
> Le nouveau mot de passe doit être conforme à la politique de mot de passe dans le module **Authentification** (voir Authentification à la page 297).

> **IMPORTANT :**
>
> Pour des raisons de sécurité, le nouveau mot de passe ne doit pas correspondre au mot de passe précédent.

Saisissez le nouveau mot de passe dans le champ **Nouveau mot de passe**.

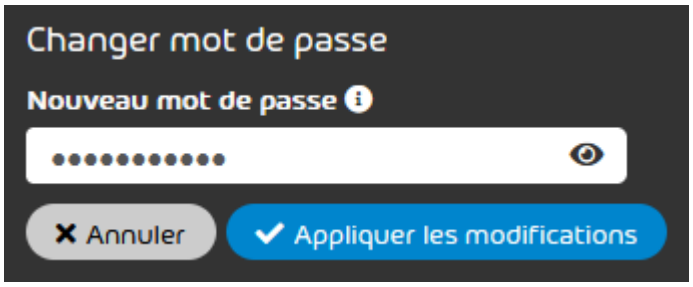


Illustration 196 : Saisir le mot de passe

7. Cliquez sur **Appliquer les modifications**.

- Le mot de passe est sauvegardé. Un message de confirmation apparaît. Pour des raisons de sécurité, l'utilisateur est notifié par courriel de la modification du mot de passe.

Le mot de passe d'une boîte aux lettres créée manuellement a été modifié.

Réinitialiser l'authentification multifacteur

Vous avez activé l'authentification multifacteur pour les utilisateurs d'un domaine (voir Activer l'authentification multifacteur à la page 301). Un utilisateur du domaine a configuré l'authentification multifacteur pour son compte du Control Panel (voir « Configurer l'authentification multifacteur » dans le manuel du Control Panel).

Si un utilisateur rencontre des problèmes avec l'authentification multifacteur (voir « Élimination des erreurs : Problèmes avec l'authentification multifacteur » dans le manuel du Control Panel), vous pouvez réinitialiser l'authentification multifacteur pour cet utilisateur. L'authentification multifacteur est alors désactivée pour l'utilisateur et sa configuration d'authentification multifacteur est supprimée.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine de l'utilisateur pour lequel vous souhaitez réinitialiser l'authentification multifacteur.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche de menu à côté de la boîte aux lettres pour laquelle vous souhaitez réinitialiser l'authentification multifacteur.

Un menu s'ouvre.

Illustration 197 : Menu

5. Cliquez sur **Réinitialiser l'authentification multifacteur**.

Un affichage étendu s'ouvre.

6. Cliquez sur **Réinitialiser l'authentification multifacteur**.

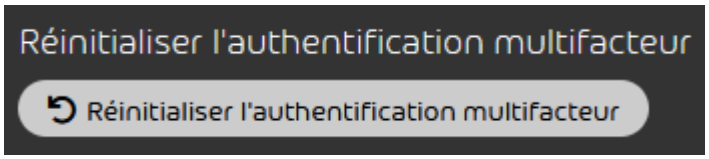


Illustration 198 : Réinitialiser l'authentification multifacteur

- Une fenêtre de confirmation s'ouvre.

7. Cliquez sur **Confirmer**.

Illustration 199 : Confirmer

- L'authentification multifacteur est désactivée pour l'utilisateur et sa configuration d'authentification multifacteur est supprimée. L'utilisateur est informé par courriel que l'authentification multifacteur a été désactivée pour son compte. L'utilisateur peut désormais se connecter au Control Panel sans utiliser l'authentification multifacteur.

L'authentification multifacteur a été réinitialisée pour un utilisateur.

L'utilisateur peut reconfigurer l'authentification multifacteur pour son compte (voir « Configurer l'authentification multifacteur » dans le manuel du Control Panel).

Supprimer une boîte aux lettres

Vous avez ajouté une boîte aux lettres au Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d'un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez supprimer les boîtes aux lettres créées manuellement (voir Types de boîtes aux lettres à la page 218) du Control Panel.

Tous les paramètres d'une boîte aux lettres sont perdus lorsque celle-ci est supprimée. Cela a pour effet les conséquences suivantes :

- La connexion au Control Panel est interrompue et les futurs courriels de la boîte aux lettres ne seront plus traités par nos services.
- Les propriétaires de boîtes aux lettres supprimées ne peuvent plus se connecter au Control Panel avec leurs identifiants.
- Les boîtes aux lettres supprimées sont retirées des groupes auxquels elles appartiennent (voir Groupes à la page 268).
- Les attributions de rôles (voir Rôles à la page 49) des utilisateurs de boîtes aux lettres supprimées sont supprimées.
- Les adresses alias (voir Ajouter une adresse alias à la page 243) des boîtes aux lettres supprimées sont supprimées.
- Les boîtes aux lettres supprimées sont supprimées des listes de redirection des boîtes aux lettres de redirection (voir Ajouter boîte aux lettres de redirection à la page 237).
- Les boîtes aux lettres retirées sont supprimées des listes de remplaçants (voir Saisir une délégation à la page 245) d'autres boîtes aux lettres. Les représentants des boîtes aux lettres supprimées sont supprimées.

Les informations sur les courriels entrants et sortants des boîtes aux lettres supprimées sont conservées dans le Control Panel et visibles pour les administrateurs ainsi que pour les utilisateurs auxquels les boîtes aux lettres supprimées ont été attribuées.

REMARQUE :

La suppression d'une boîte aux lettres du Control Panel n'influence que les données et les paramètres qui sont enregistrés dans le Control Panel pour cette boîte aux lettres. La boîte aux lettres elle-même est conservée.

IMPORTANT :

Les boîtes aux lettres les boîtes aux lettres LDAP ne peuvent être importées manuellement depuis le Control Panel.

REMARQUE :

Au lieu de supprimer les boîtes aux lettres une par une, les administrateurs peuvent en supprimer plusieurs simultanément (voir Supprimer plusieurs boîtes aux lettres à la page 265).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer une boîte aux lettres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur la flèche de menu de la boîte aux lettres désirée.

Illustration 200 : Ouvrir le menu

- Un menu s'ouvre.

5. Cliquez sur **Éliminer**.

- Une fenêtre de confirmation s'ouvre.

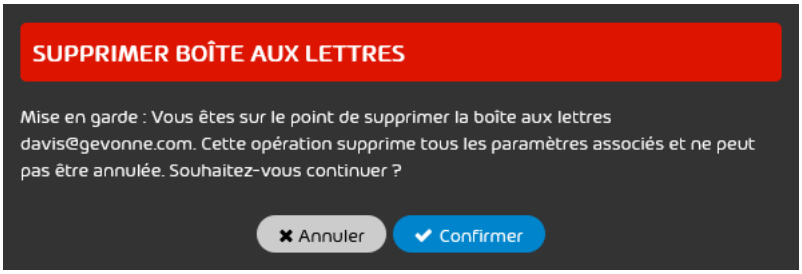


Illustration 201 : Supprimer la boîte aux lettres

6. Cliquez sur **Confirmer**.

La boîte aux lettres est supprimée du Control Panel. Un message de confirmation apparaît.

Une boîte aux lettres créée manuellement a été supprimée du Control Panel.

Supprimer plusieurs boîtes aux lettres

Vous avez ajouté des boîtes aux lettres dans le Control Panel (voir Ajouter une boîte aux lettres à la page 220 et Importer des boîtes aux lettres à partir d' un fichier CSV à la page 223).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez supprimer simultanément du Control Panel plusieurs boîtes aux lettres créées manuellement (voir Types de boîtes aux lettres à la page 218).

Tous les paramètres d'une boîte aux lettres sont perdus lorsque celle-ci est supprimée. Cela a pour effet les conséquences suivantes :

- La connexion au Control Panel est interrompue et les futurs courriels de la boîte aux lettres ne seront plus traités par nos services.
- Les propriétaires de boîtes aux lettres supprimées ne peuvent plus se connecter au Control Panel avec leurs identifiants.
- Les boîtes aux lettres supprimées sont retirées des groupes auxquels elles appartiennent (voir Groupes à la page 268).
- Les attributions de rôles (voir Rôles à la page 49) des utilisateurs de boîtes aux lettres supprimées sont supprimées.
- Les adresses alias (voir Ajouter une adresse alias à la page 243) des boîtes aux lettres supprimées sont supprimées.
- Les boîtes aux lettres supprimées sont supprimées des listes de redirection des boîtes aux lettres de redirection (voir Ajouter boîte aux lettres de redirection à la page 237).
- Les boîtes aux lettres retirées sont supprimées des listes de remplaçants (voir Saisir une délégation à la page 245) d'autres boîtes aux lettres. Les représentants des boîtes aux lettres supprimées sont supprimées.

Les informations sur les courriels entrants et sortants des boîtes aux lettres supprimées sont conservées dans le Control Panel et visibles pour les administrateurs ainsi que pour les utilisateurs auxquels les boîtes aux lettres supprimées ont été attribuées.

REMARQUE :

La suppression d'une boîte aux lettres du Control Panel n'influence que les données et les paramètres qui sont enregistrés dans le Control Panel pour cette boîte aux lettres. La boîte aux lettres elle-même est conservée.

IMPORTANT :

Les boîtes aux lettres les boîtes aux lettres LDAP ne peuvent être importées manuellement depuis le Control Panel.

REMARQUE :

Au lieu de supprimer plusieurs boîtes aux lettres simultanément, les administrateurs peuvent supprimer les boîtes aux lettres individuellement.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer des boîtes aux lettres.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Cliquez sur en haut du module.

Une colonne avec des cases à cocher s'affiche dans la liste des domaines.

5. Cochez les cases des boîtes aux lettres que vous souhaitez supprimer.

Illustration 202 : Sélectionner les boîtes aux lettres

- Le bouton **Éliminer** est déverrouillé.

6. Cliquez sur **Éliminer**.

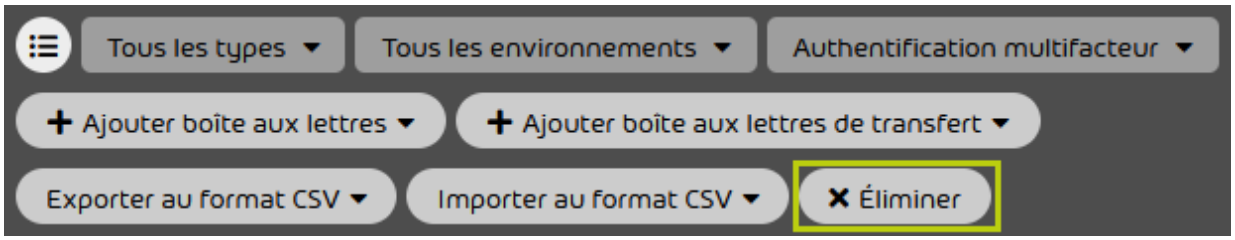


Illustration 203 : Supprimer les boîtes aux lettres

- Une fenêtre de confirmation apparaît.

7. Cliquez sur **Confirmer**.

Illustration 204 : Confirmer la suppression

Les boîtes aux lettres sont supprimées du Control Panel. La suppression s'effectue en arrière-plan et peut prendre quelques minutes.

Plusieurs boîtes aux lettres créées manuellement ont été supprimées du Control Panel.

Groupes

Dans le Control Panel, les boîtes aux lettres peuvent être rassemblées en groupes. Certains services du Control Panel peuvent être appliqués uniquement à des groupes. D'autres services autorisent au moins les réglages pour un groupe. C'est pour cette raison que les groupes facilitent la configuration des services dans le Control Panel.

Dans le module **Paramètres client** > **Groupes**, les administrateurs côté clientspeuvent créer des groupes et ajouter des membres individuels (voir Créer un groupe à la page 270) et gérer les groupes existants. Les listes de membres d'un groupe déjà existantes peuvent être importées sous forme de fichier CSV (voir Importer des membres de groupe à partir d' un fichier CSV à la page 271). Pour ce fichier CSV, des consignes particulières s'appliquent (voir Fichiers CSV pour importer des membres de groupe à la page 276). Il est également possible d'exporter des listes de membres de groupes existants sous forme de fichiers CSV (voir Exporter des groupes sous un fichier CSV à la page 282).

REMARQUE :

L'appartenance à un groupe des boîtes aux lettres Microsoft 365 (voir le chapitre « Types de boîtes aux lettres » dans le manuel 365 Total Protection) est gérée exclusivement dans Microsoft 365. Par conséquent, les boîtes aux lettres Microsoft 365 ne peuvent pas être ajoutées à des groupes depuis le Control Panel. Toutefois, il est possible de reproduire des groupes de Microsoft 365 dans le Control Panel en créant des groupes portant les mêmes noms dans le Control Panel. Pour plus d'informations concernant la synchronisation de groupes dans Microsoft 365, voir le chapitre « Synchroniser des groupes de Microsoft 365 dans le Control Panel » dans le manuel 365 Total Protection.

Pour gérer les groupes, les administrateurs côté clients disposent des options suivantes dans le menu des groupes.

Tableau 18 : Gérer les groupes

SYMBOLE	DÉSIGNATION	DESCRIPTION
	Détails	Informations détaillées sur le groupe
	Gérer les membres	Ajouter/supprimer des membres (voir Gérer les membres à la page 277)
	Modifier nom	Modification du nom du groupe (voir Renommer un groupe à la page 279)
	Modifier la description	Modification de la description du groupe (voir Modifier la description du groupe à la page 280)
	Supprimer	Supprimer groupe (voir Supprimer un groupe à la page 284)

Créer un groupe

Dans le module **Paramètres client** > **Groupes**, vous pouvez créer un nouveau groupe à partir des boîtes aux lettres existantes .

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer un groupe.
3. Naviguez vers **Paramètres client** > **Groupes**.
4. Cliquez sur **Ajouter**.

Un menu déroulant s'ouvre.

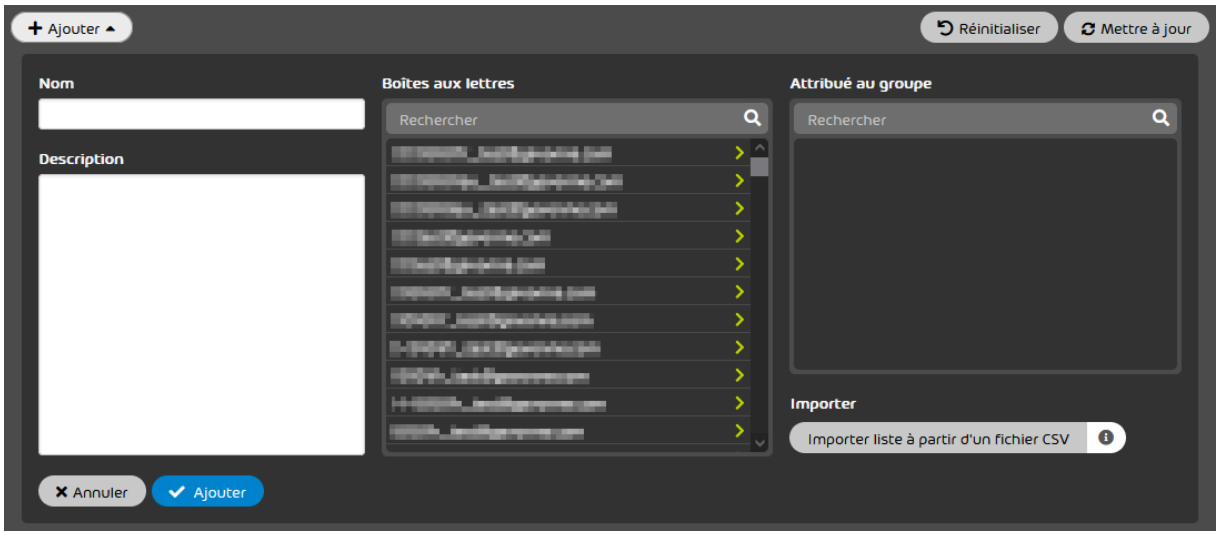


Illustration 205 : Ajouter un nouveau groupe

5. Sous **Nom**, attribuez un nom de groupe.
6. Facultatif : Décrivez le groupe dans le champ **Description**.

7. Ajoutez des boîtes aux lettres au nouveau groupe. Vous avez deux options :

   - Dans **Boîtes aux lettres**, sélectionnez au moins une boîte aux lettres qui doit être ajoutée au groupe. Pour ajouter une boîte aux lettres au groupe, cliquez sur la boîte aux lettres.

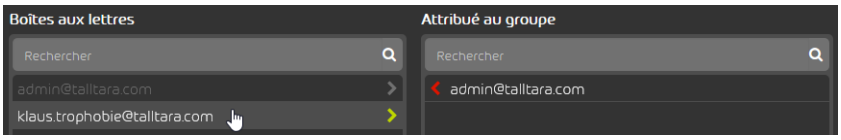


Illustration 206 : Ajouter une seule boîte aux lettres

   - Importez une liste de membres déjà existante à partir d'un fichier CSV (voir Importer des membres de groupe à partir d' un fichier CSV à la page 271). Vous pouvez importer uniquement les membres pour un groupe unique à chaque importation.

Les boîtes aux lettres sélectionnées ou importées apparaissent sous **Attribué au groupe**.

8. Cliquez sur **Ajouter**.

Le groupe est enregistré. Les boîtes aux lettres sous **Attribué au groupe** sont attribuées au groupe.

Un groupe a été créé.

Vous pouvez ensuite gérer les membres du groupe (voir Gérer les membres à la page 277 et Importer des membres de groupe à partir d' un fichier CSV à la page 271), renommer le groupe (voir Renommer un groupe à la page 279), adapter la description du groupe (voir Modifier la description du groupe à la page 280), exporter le groupe sous un fichier CSV (voir Exporter des groupes sous un fichier CSV à la page 282) ou supprimer le groupe (voir Supprimer un groupe à la page 284).

Importer des membres de groupe à partir d' un fichier CSV

Au lieu d'affecter manuellement des utilisateurs à un groupe, vous pouvez ajouter des utilisateurs à l'aide d'une liste CSV dans le module **Paramètres client** > **Groupes**. Vous pouvez affecter des utilisateurs à des groupes nouvellement créés et à des groupes existants en utilisant une liste CSV.

REMARQUE :

Vous pouvez importer uniquement les membres pour un groupe unique à chaque importation.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez importer des membres de groupe.
3. Naviguez vers **Paramètres client** > **Groupes**.
4. Vous avez deux possibilités :
   - Créer un nouveau groupe et importer des membres à partir d'un fichier CSV (voir Section a)
   - Ajouter des membres à partir d'un fichier CSV à un autre groupe existant (voir Section b)

a) Cliquez sur **Ajouter**.

Un formulaire apparaît.

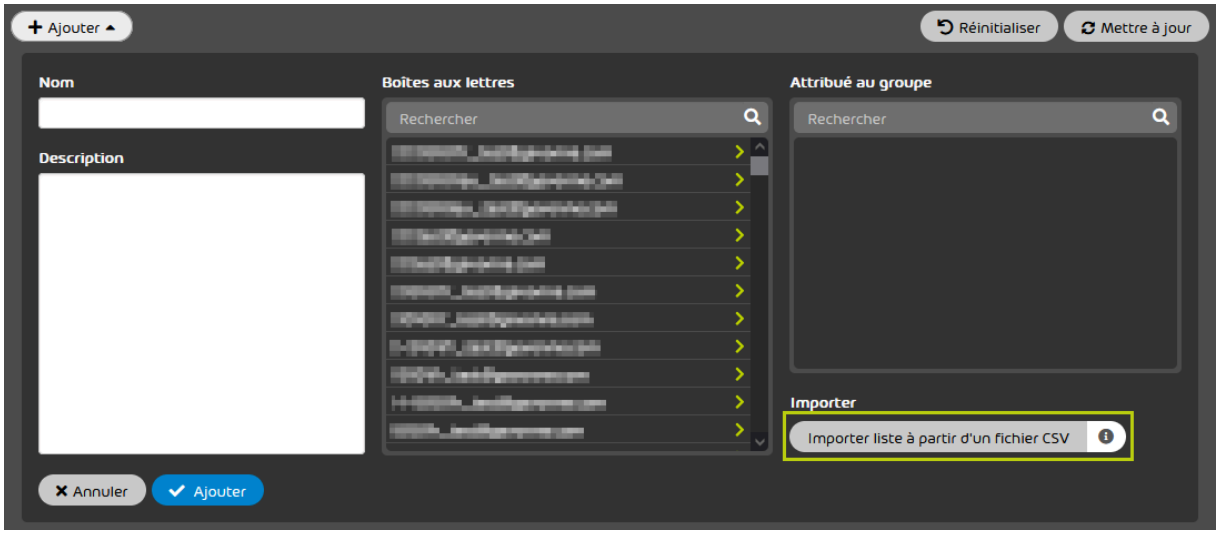


Illustration 207 : Importer des membres de groupe à partir d' un fichier CSV pour un nouveau groupe

b) Sélectionnez le groupe existant dans la partie inférieure de la page et cliquez sur **Gérer les membres**.

Un formulaire apparaît.

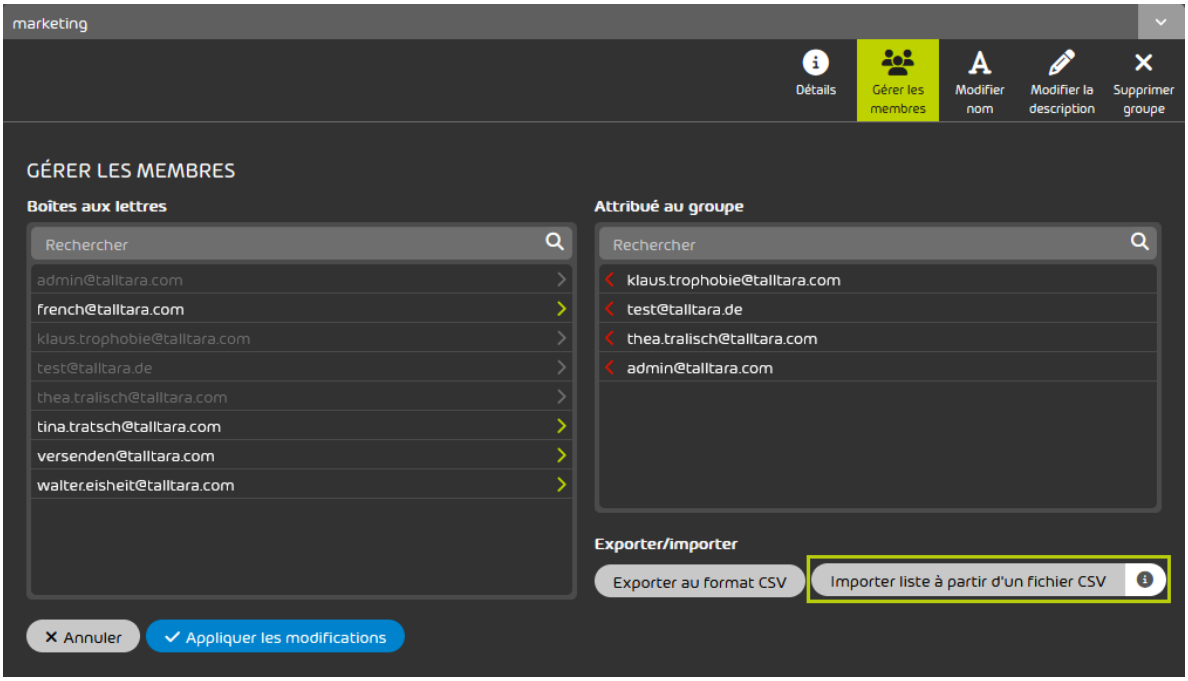


Illustration 208 : Importer des membres de groupe à partir d' un fichier CSV pour un groupe existant

5. Cliquez sur **Importer liste à partir d'un fichier CSV**.

> **REMARQUE :**
>
> Seuls sont importés à partir du fichier CSV les membres de groupe pour le groupe actuellement sélectionné.

Une fenêtre de sélection des fichiers s'ouvre.

6. Sélectionnez le fichier CSV désiré.

> **IMPORTANT :**
>
> Pour s'assurer qu'un fichier CSV externe avec des membres de groupe peut être importé dans le Control Panel sans erreur, des règles spéciales doivent être observées concernant le format du fichier, sa structure de contenu et une syntaxe valide (voir Fichiers CSV pour importer des membres de groupe à la page 276).

Tous les membres de groupe qui ont été lus s'affichent depuis le fichier CSV s'affichent sous **Attribué au groupe**.

> **REMARQUE :**
>
> Les règles suivantes s'appliquent pour l'importation de membres de groupe depuis les fichiers CSV#:
>
> - Les membres de groupe qui ont été attribués à un autre groupe sont également importés depuis un fichier CSV. Les membres de groupe s'affichent sous **Attribué au groupe**.
> - Si les entrées sont lues depuis plusieurs fichiers CSV, des entrées en doublon sont identifiées automatiquement dans les différents fichiers CSV. Les entrées en doublon sont importées une seule fois et s'affichent sous **Attribué au groupe**.
> - Les entrées en doublon dans un fichier CSV unique sont importées une seule fois et s'affichent sous **Attribué au groupe**.
> - Les entrées non valides sont également importées depuis un fichier CSV et s'affichent sous **Attribué au groupe**. Dès que vous enregistrez le groupe, on vérifie si les entrées de la liste sont valides. Si la liste contient des entrées non valides, un message d'erreur apparaît. Supprimez toutes les entrées non valides (voir Fichiers CSV pour importer des membres de groupe à la page 276) et enregistrez le groupe.

7. Cliquez sur **Ajouter** ou **Appliquer les modifications** pour enregistrer vos modifications.

Le groupe est enregistré.

IMPORTANT :

Si la liste contient des membres de groupe d'autres groupes ou des entrées non valide sous **Attribué au groupe**, un message d'erreur apparaît. Supprimez les membres de groupe des autres groupes et les entrées non valides de la liste, et enregistrez le groupe.

Des membres de groupe ont été importés depuis un fichier CSV et ajoutés à un groupe.

Fichiers CSV pour importer des membres de groupe

Pour garantir qu'un fichier CSV externe contenant des informations sur les membres du groupe puisse être importé dans le Control Panel sans erreur (voir Importer des membres de groupe à partir d'un fichier CSV à la page 271), des règles spéciales doivent être observées pour l'extension des fichiers et la structure du contenu.

Règles de structure d'un fichier CSV pour l'importation des membres du groupe

- L'extension du fichier à importer est toujours **.csv**. Les autres extensions de fichier telles que .txt ou .docx ne sont pas autorisées et ne seront pas acceptées.
- Le fichier CSV ne contient qu'une seule colonne dans laquelle les entrées individuelles sont saisies l'une après l'autre.
- La première ligne est toujours le nom de la colonne et peut être nommée individuellement.
- Les membres du groupe sont répertoriés par leur adresse courriel. Les adresses doivent être bien formées (selon le modèle « partielocale@nomhote.domaine-principal »).

IMPORTANT :

Les adresses mal formées ne sont pas prises en compte lors de l'importation.

- Chaque ligne ne peut contenir qu'une seule adresse.
- Les doublons n'ont aucune influence sur le traitement du fichier, mais doivent être évités.

Gérer les membres

Vous avez créé un groupe (voir Créer un groupe à la page 270).

Dans le module **Paramètres client** > **Groupes**, vous pouvez ajouter des boîtes aux lettres créées manuellement (voir Types de boîtes aux lettres à la page 218) à des groupes ou les supprimer de groupes. Dans ce cas, le fait que le groupe soit synchronisé ou non n'a aucune importance.

REMARQUE :

Les les boîtes aux lettres LDAP ne peuvent pas être ajoutées à des groupes ou supprimées de groupes dans le Control Panel. Votre appartenance à un groupe est gérée exclusivement dans le service d'annuaire.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez gérer les membres de groupe.
3. Naviguez vers **Paramètres des clients** > **Groupes** et cliquez sur la flèche de menu du groupe souhaité.

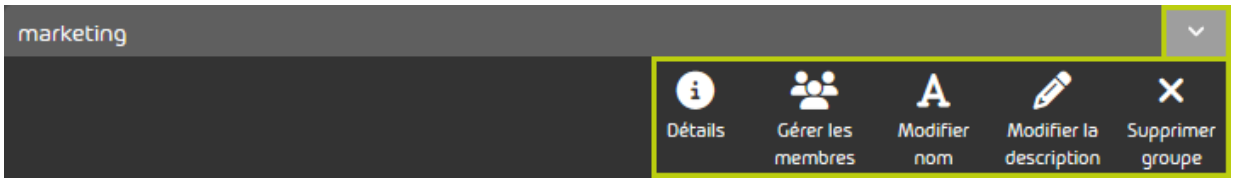


Illustration 209 : Ouvrir le menu de groupes

4. Cliquez sur **Gérer les membres**.

Un menu déroulant avec deux fenêtres s'ouvre dans lequel toutes les boîtes aux lettres enregistrées (à gauche) et toutes les boîtes aux lettres affectées au groupe (à droite) sont affichées.

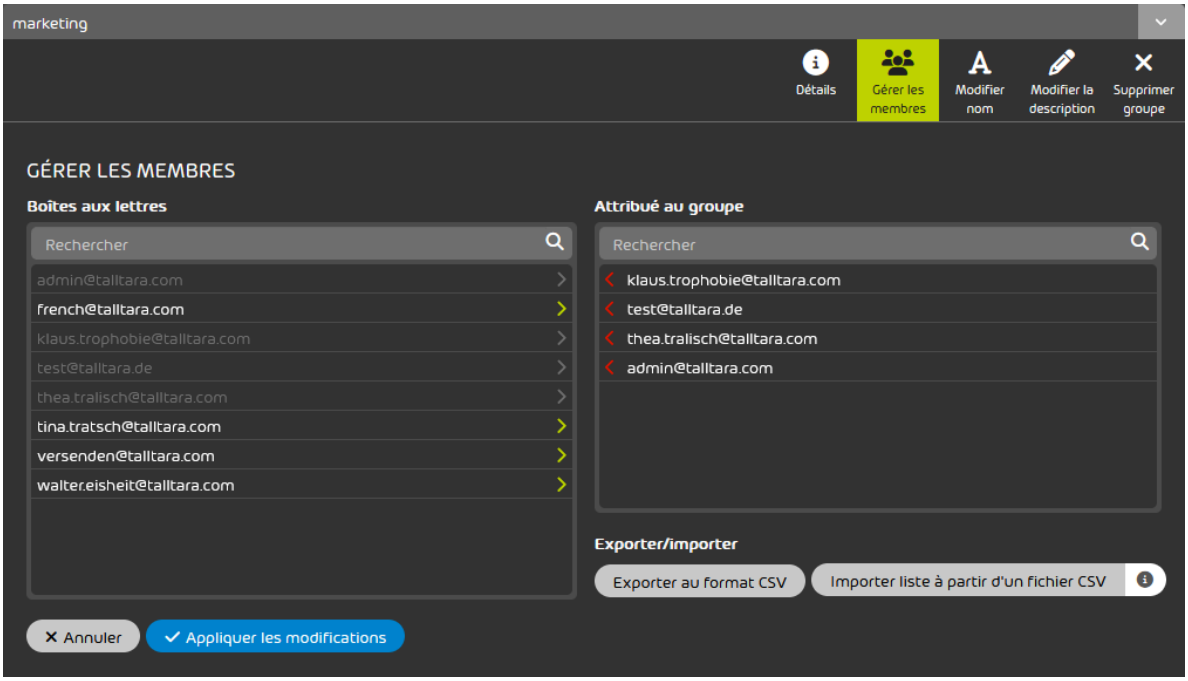


Illustration 210 : Gérer les membres du groupe

5. Gérez les membres d'un groupe :

   - Si vous souhaitez ajouter d'autres membres au groupe, cliquez dans le tableau **Boîtes aux lettres** (à gauche) sur les membres à ajouter. Les listes de groupes déjà existantes peuvent être importées ici sous forme de fichiers CSV (voir Importer des membres de groupe à partir d' un fichier CSV à la page 271).
   - Si vous souhaitez supprimer du groupe des membres existants, cliquez dans le tableau **Attribué au groupe** (à droite) sur les membres du groupe à supprimer.

   REMARQUE :

   Les les boîtes aux lettres LDAP apparaissent en gris dans les tableaux **Boîtes aux lettres** et **Attribué au groupe** et ne peuvent pas être déplacées d'un tableau à l'autre.

Les membres sont ajoutés au groupe ou supprimés du groupe.

6. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées dans le Control Panel.

> **REMARQUE :**
>
> Les modifications apportées aux groupes synchronisés ne sont pas appliquées dans le service d'annuaire pendant la synchronisation, mais sont conservées dans le Control Panel.

Les membres du groupe ont été gérés.

Renommer un groupe

Vous avez créé un groupe (voir Créer un groupe à la page 270).

Sous **Paramètres client** > **Groupes**, vous pouvez renommer des groupes (voir Groupes à la page 268).

> **IMPORTANT :**
>
> Les groupes qui sont synchronisés avec un service d'annuaire ne sont plus synchronisés après que ceux-ci ont été renommés.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine dont vous souhaitez renommer le groupe.
3. Naviguez vers **Paramètres des clients** > **Groupes** et cliquez sur la flèche de menu du groupe souhaité.

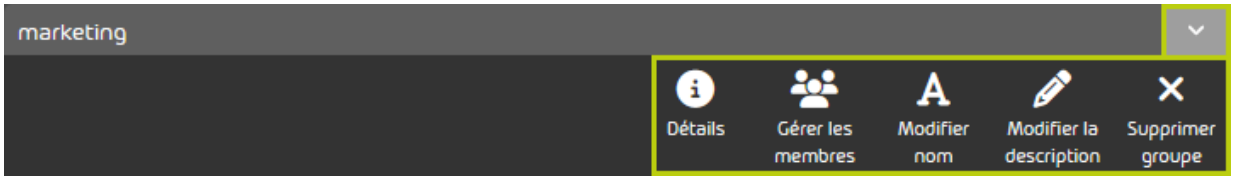
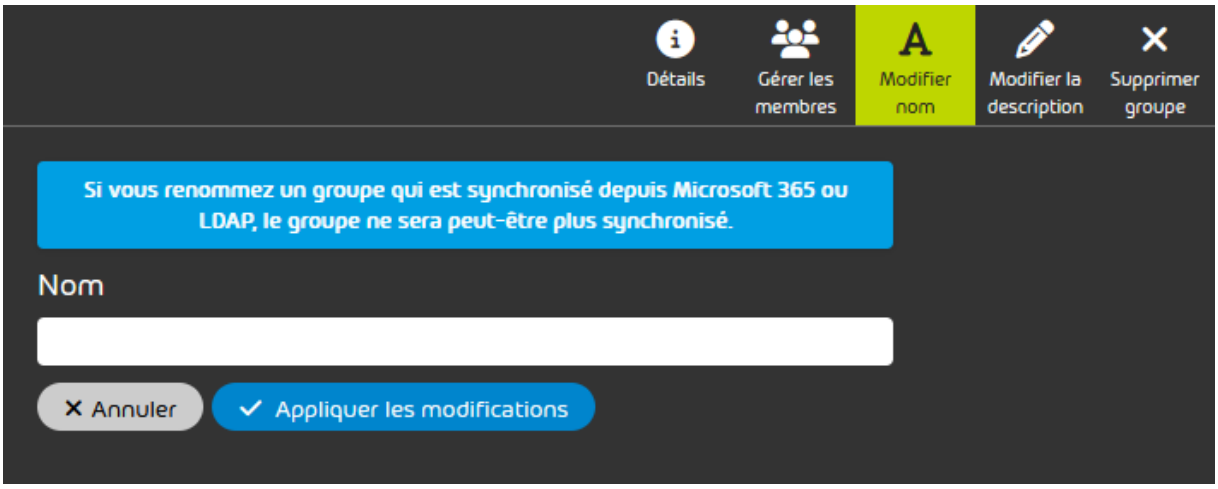


Illustration 211 : Ouvrir le menu de groupes

4. Cliquez sur **Modifier nom**.

Un menu déroulant s'ouvre.



5. **IMPORTANT :**

   Si un groupe qui n'est pas encore synchronisé reçoit le nom d'un groupe de d'un service d'annuaire synchronisé via LDAP, le groupe sera désormais synchronisé. Des boîtes aux lettres synchronisées, attribuées au groupe dans au service d'annuaire, sont attribuées au groupe dans le Control Panel. L'appartenance au groupe des boîtes aux lettres synchronisées est synchronisée en permanence. Les boîtes aux lettres non synchronisées qui ont été manuellement attribuées au groupe dans le Control Panel restent attribuées au groupe et ne seront pas prises en compte lors des synchronisations.

   Saisissez le nouveau nom du groupe dans le champ de saisie.

6. Cliquez sur **Appliquer les modifications**.

Un groupe a été renommé.

Modifier la description du groupe

Vous avez créé un groupe (voir Créer un groupe à la page 270).

Dans le module **Paramètres client** > **Groupes**, vous pouvez modifier les descriptions des groupes.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine du groupe dont vous souhaitez modifier la description.
3. Naviguez vers **Paramètres des clients** > **Groupes** et cliquez sur la flèche de menu du groupe souhaité.

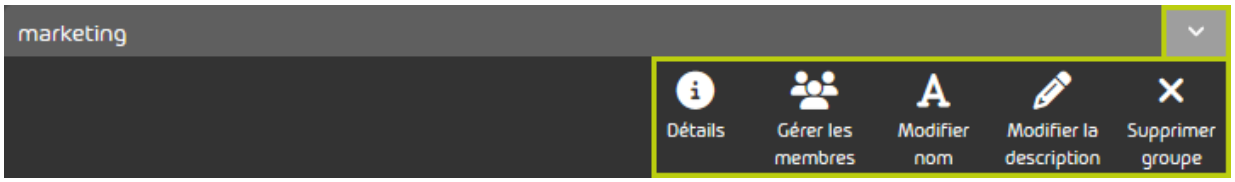
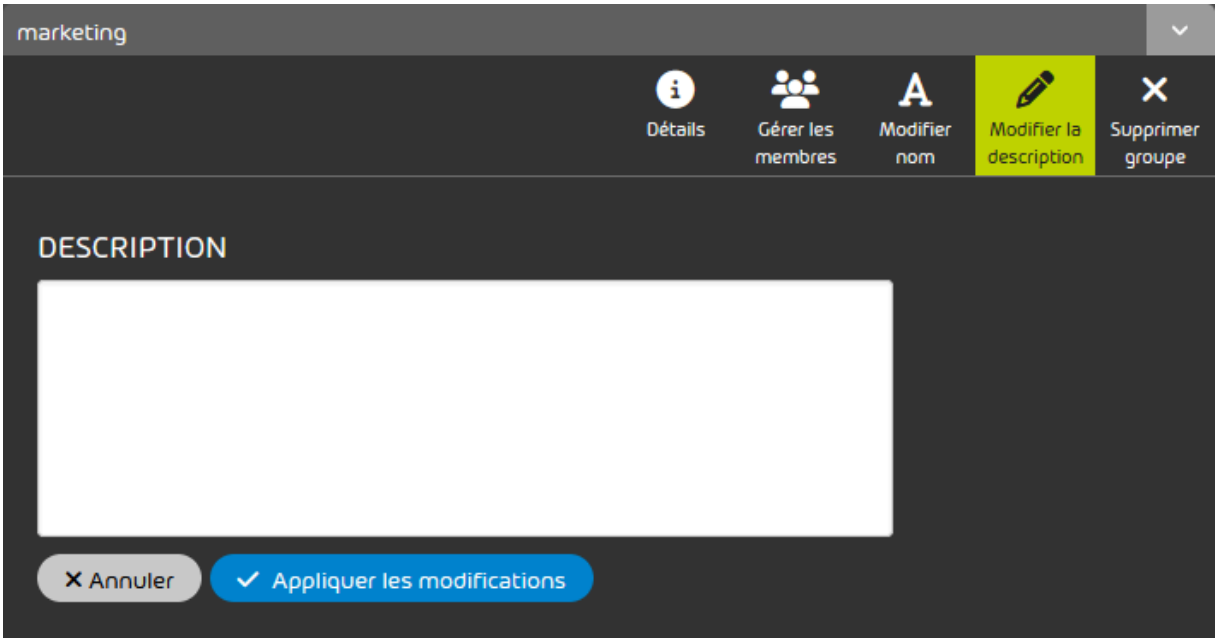


Illustration 212 : Ouvrir le menu de groupes

4. Cliquez sur **Modifier la description**.

Un menu déroulant s'ouvre.



5. Saisissez la description désirée pour le groupe et cliquez sur **Appliquer les modifications**.

Une description de groupe a été modifiée.

Exporter des groupes sous un fichier CSV

Vous avez créé un groupe (voir Créer un groupe à la page 270).

Dans le module **Paramètres client** > **Groupes**, vous pouvez exporter des groupes sous un fichier CSV.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Groupes**.
4. Cliquez sur **Exporter au format CSV**.

Un affichage étendu s'ouvre.

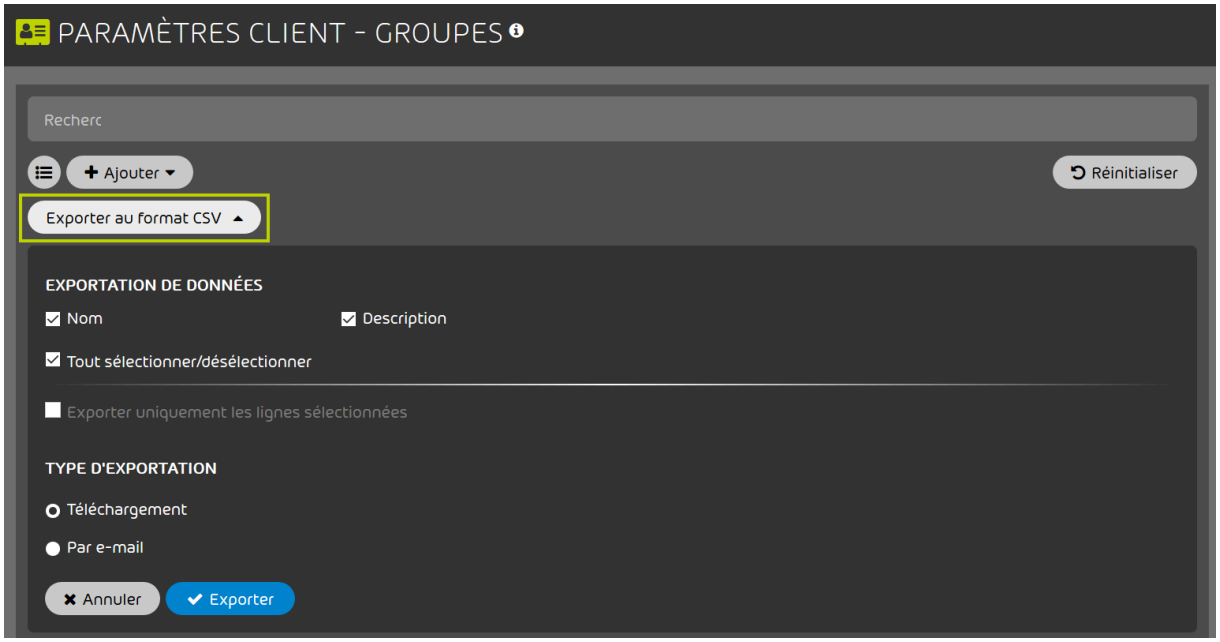


Illustration 213 : Sélectionner les données à exporter

5. Sous **Exportation de données**, cochez les cases des données que vous souhaitez exporter.
   - **Nom** : les noms des groupes sont exportés.
   - **Description** : la description des groupes est exportée.
   - **Sélectionner/désélectionner tout** : toutes les cases décrites au préalable sont sélectionnées ou désélectionnées.
6. Facultatif : Si vous souhaitez exporter uniquement les données de groupes sélectionnés, procédez comme suit :

   a) Cliquez sur en haut du module.

Une colonne avec des cases à cocher s'affiche dans le tableau.

   b) Cochez la case des lignes à partir desquelles vous souhaitez exporter des données.

Illustration 214 : Sélectionner des lignes

Dans l'affichage étendu, la case à cocher **Exporter uniquement les lignes sélectionnées** est déverrouillée.

   c) Cochez la case déverrouillée **Exporter uniquement les lignes sélectionnées**.

Illustration 215 : Exporter les lignes sélectionnées

7. Facultatif : Sous **Exportation de données**, sélectionnez si vous souhaitez exporter les deux colonnes **Nom** et **Description**.

Illustration 216 : Sélectionner des colonnes

8. Sous **Type d'exportation**, sélectionnez si le fichier CSV doit être mis à disposition en téléchargement ou envoyé par courriel.
   - **Téléchargement** : le fichier CSV est mis à disposition dans les téléchargements.
   - **Par courriel** : le fichier CSV est envoyé par courriel.

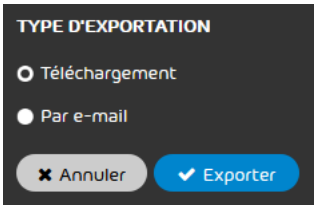


Illustration 217 : Sélectionner le type d' exportation

9. Cliquez sur **Exporter**.

Les données d'un groupe ont été exportées sous un fichier CSV.

Supprimer un groupe

Vous avez créé un groupe (voir Créer un groupe à la page 270).

Dans le module **Paramètres client** > **Groupes**, vous pouvez supprimer un groupe existant (voir Groupes à la page 268).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer un groupe.

3. Naviguez vers **Paramètres des clients** > **Groupes** et cliquez sur la flèche de menu du groupe souhaité.

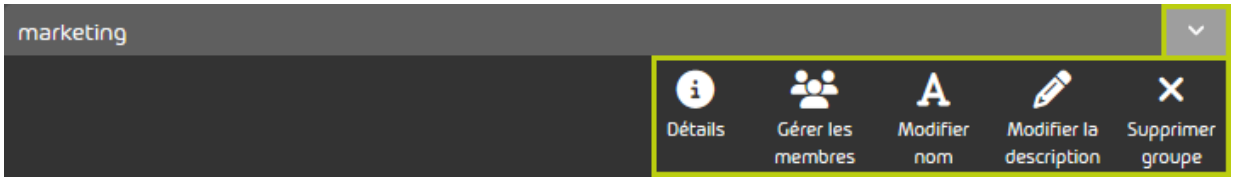
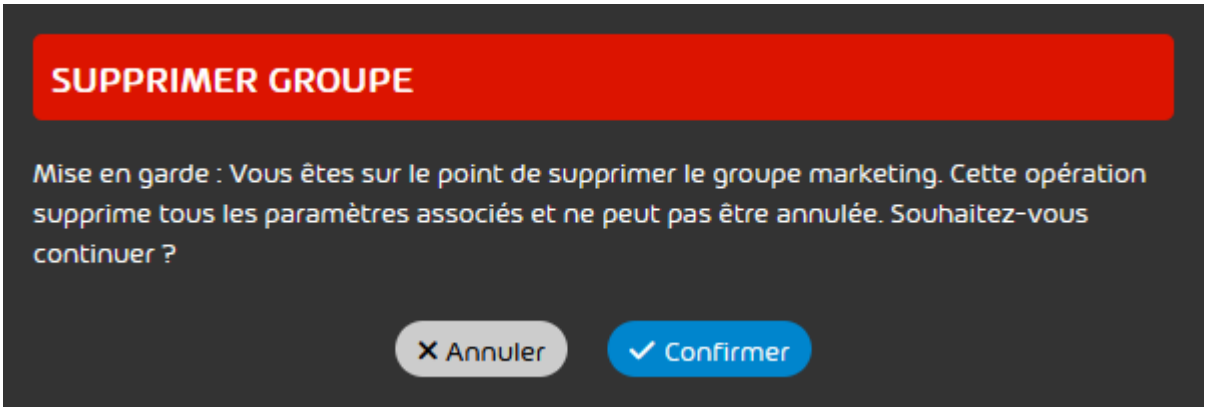


Illustration 218 : Ouvrir le menu de groupes

4. Cliquez sur **Confirmer**.

> **PRUDENCE :**
>
> En supprimant le groupe, tous les paramètres et les membres du groupe sont supprimés définitivement.

Un avertissement apparaît.



5. Confirmez l'avertissement en appuyant sur **Confirmer**.

Un groupe a été supprimé.

Domaines

Le module **Paramètres client** > **Domaines** permet d'afficher le domaine principal et les domaines d'alias d'un client.

REMARQUE :

Les domaines d'alias peuvent par exemple être utilisés s'il existe différents domaines top level pour un domaine. Un administrateur peut par exemple ajouter **domaineclient.com** pour le domaine principal, **.de** et **.es** pour les domaines top level. Dans ce cas, **domaineclient.de** et **domaineclient.es** seraient les domaines d'alias du domaine principal.

Nous ne facturons aucun frais pour les domaines d'alias.

Dans ce module (voir Supprimer un domaine alias à la page 292), les administrateurs côté clients peuvent créer de nouveaux domaines d'alias (voir Ajouter un domaine d'alias à la page 286) et supprimer des domaines d'alias existants. Le domaine principal ne peut pas être supprimé. En outre, les administrateurs peuvent exporter les domaines affichés au format CSV (voir Exporter des domaines en tant que fichier CSV à la page 290) et importer de nouveaux domaines d'alias à partir de fichiers CSV (voir Importer des domaines d'alias à partir d'un fichier CSV à la page 288). Pour ce fichier CSV, des consignes particulières s'appliquent (voir Fichiers CSV pour importer des domaines d'alias à la page 289).

Pour des raisons de sécurité, nous vérifions si un client est autorisé à gérer les domaines enregistrés dans le Control Panel (voir Vérifications de domaines à la page 294).

Ajouter un domaine d'alias

Dans le module **Paramètres client** > **Domaines**, vous pouvez, en tant qu'administrateur côté client, ajouter des domaines d'alias au domaine principal d'un client. La procédure décrite ici vous permet d'ajouter des domaines d'alias individuellement. Vous pouvez également importer une liste de domaines alias à partir d'un fichier CSV (voir Importer des domaines d'alias à partir d'un fichier CSV à la page 288).

REMARQUE :

Les domaines d'alias peuvent par exemple être utilisés s'il existe différents domaines top level pour un domaine. Un administrateur peut par exemple ajouter **domaineclient.com** pour le domaine principal, **.de** et **.es** pour les domaines top level. Dans ce cas, **domaineclient.de** et **domaineclient.es** seraient les domaines d'alias du domaine principal.

Nous ne facturons aucun frais pour les domaines d'alias.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client pour qui vous souhaitez ajouter un domaine d'alias au domaine principal.
3. Naviguez vers **Paramètres client** > **Domaines**.
4. Cliquez sur **Ajouter domaine**.

D'autres paramètres apparaissent.

5. **IMPORTANT :**

   Le domaine d'alias doit être un domaine valide.

   Saisissez le domaine d'alias dans le champ **Domaine**.

6. Cliquez sur **Ajouter**.

Le domaine d'alias est ajouté à la liste des domaines. Le domaine d'alias apparaît dans la colonne **Vérifié** à côté du statut **Pas vérifié**. Après quelques minutes, une vérification permet d'établir si le domaine alias peut être vérifié (voir Vérifications de domaines à la page 294).

Un domaine d'alias a été ajouté au domaine principal d'un client.

Vous pouvez ensuite exporter les domaines du client en tant que fichier CSV (voir Exporter des domaines en tant que fichier CSV à la page 290) ou supprimer les domaines alias (voir Supprimer un domaine alias à la page 292).

Importer des domaines d'alias à partir d'un fichier CSV

Au lieu d'ajouter les domaines d'alias individuellement à un domaine principal (voir Ajouter un domaine d'alias à la page 286), vous pouvez importer des domaines d'alias à partir d'une liste CSV dans le module **Paramètres client** > **Domaines**. Vous pouvez importer des domaines d'alias aussi bien initialement, si aucune donnée n'a encore été saisie, qu'en cours de fonctionnement via une liste CSV.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client pour quoi vous souhaitez ajouter les domaines d'alias au domaine principal.
3. Naviguez vers **Paramètres client** > **Domaines**.
4. Cliquez sur **Importer liste à partir d'un fichier CSV**.

Une fenêtre de sélection des fichiers s'ouvre.

5. Sélectionnez le fichier CSV désiré.

> **IMPORTANT :**
>
> Pour s'assurer qu'un fichier CSV externe avec des domaines d'alias peut être importé dans le Control Panel sans erreur, des règles spéciales doivent être observées concernant le format du fichier, sa structure de contenu et une syntaxe valide (voir Fichiers CSV pour importer des domaines d'alias à la page 289).

Si le fichier CSV contient des domaines d'alias qui ne sont pas encore disponibles dans le Control Panel, ils seront ajoutés à la liste de domaines.

Les domaine d'alias sont importées depuis un fichier CSV et ajoutés au domaine principal du client.

Vous pouvez ensuite exporter les domaines du client en tant que fichier CSV (voir Exporter des domaines en tant que fichier CSV à la page 290) ou supprimer les domaines d'alias (voir Supprimer un domaine alias à la page 292).

Fichiers CSV pour importer des domaines d'alias

Pour garantir qu'un fichier CSV externe contenant des domaines d'alias puisse être importé dans le Control Panel sans erreur (voir Importer des domaines d'alias à partir d'un fichier CSV à la page 288), des règles spéciales doivent être observées pour l'extension des fichiers et la structure du contenu.

Règles de structure d'un fichier CSV pour l'importation de domaines d'alias

- L'extension du fichier à importer est toujours **.csv**. Les autres extensions de fichier telles que .txt ou .docx ne sont pas autorisées et ne seront pas acceptées.
- Le fichier CSV ne contient qu'une seule colonne dans laquelle les entrées individuelles sont saisies l'une après l'autre.
- La première ligne est toujours le nom de la colonne et peut être nommée individuellement.

- Les noms de domaines doivent être bien formatés.

> **IMPORTANT :**
>
> Les noms de domaines mal formatés entraînent l'annulation immédiate de l'importation. Même les entrées correctes ne seront pas importées en cas d'annulation.

- Chaque ligne ne peut contenir qu'un seul nom de domaine.
- Il ne doit y avoir aucun doublon.

> **IMPORTANT :**
>
> Les doublons entraînent l'annulation immédiate de l'importation. Même les entrées correctes ne seront pas importées en cas d'annulation.

Exporter des domaines en tant que fichier CSV

Dans le module **Paramètres client** > **Domaines**, vous pouvez exporter les domaines d'un client en tant que fichier CSV. Le fichier CVS exporté contient deux colonnes. La première colonne contient le nom des domaines. La deuxième colonne contient les types des domaines. Le domaine principal et les domaines alias sont différenciés. Vous pouvez exporter tous les domaines du client ou seulement les domaines sélectionnés.

> **REMARQUE :**
>
> Les fichiers CSV exportés ne peuvent pas être utilisés pour importer des domaines alias (voir Importer des domaines d'alias à partir d'un fichier CSV à la page 288 et Fichiers CSV pour importer des domaines d'alias à la page 289).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client dont vous souhaitez exporter le domaine.
3. Naviguez vers **Paramètres client** > **Domaines**.
4. Cliquez sur **Exporter au format CSV**.

Les paramètres pour l'exportation CSV sont affichés.

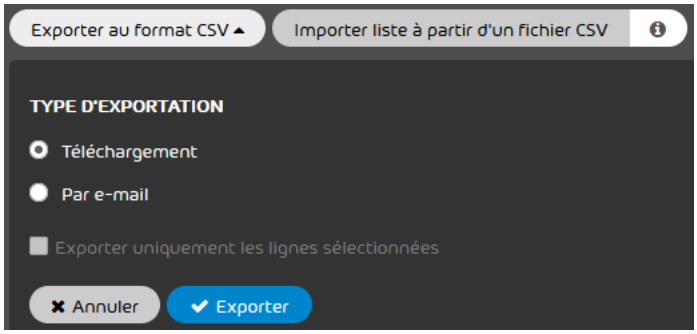


Illustration 219 : Paramètres pour l' exportation CSV

5. Facultatif : Si vous souhaitez exporter uniquement les domaines sélectionnés, procédez comme suit :

   a) Cliquez sur en haut du module.

- Une colonne avec des cases à cocher s'affiche dans la liste des domaines.

   b) Cochez les cases des lignes que vous souhaitez exporter.

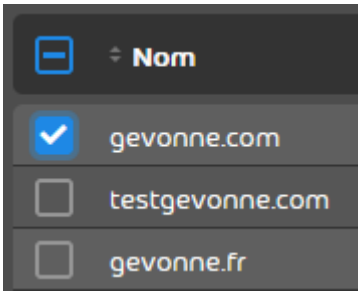


Illustration 220 : Sélectionner les lignes

- Dans les paramètres pour l'exportation CSV, la case **Exporter uniquement les lignes sélectionnées** est cochée.

   c) Cochez la case **Exporter uniquement les lignes sélectionnées**.

Illustration 221 : Exporter les lignes sélectionnées

6. Sous **Type d'exportation**, indiquez si le fichier CSV doit être mis à disposition en téléchargement ou envoyé par courriel.
   - **Téléchargement** : le fichier CSV est mis à disposition dans les téléchargements.
   - **Par courriel** : le fichier CSV est envoyé par courriel.

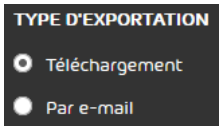


Illustration 222 : Sélectionner le type d'exportation

Si l'option **Par courriel** a été sélectionnée, un champ de saisie s'affiche.

7. Si vous avez sélectionné l'option **Par courriel**, saisissez l'adresse courriel à laquelle le fichier CSV doit être envoyé dans le champ de saisie.
8. Cliquez sur **Exporter**.

Les domaines sont exportés comme fichier CSV. Le fichier CSV est mis à disposition dans les téléchargements ou envoyé par courriel.

Tous les domaines d'un client ou les domaines sélectionnés ont été exportés comme fichier CSV.

Supprimer un domaine alias

Vous avez ajouté des domaines alias au domaine principal du client (voir Ajouter un domaine d'alias à la page 286 et Importer des domaines d'alias à partir d'un fichier CSV à la page 288).

Vous pouvez supprimer des domaines d'alias existants d'un client à partir du Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le client pour lequel vous souhaitez supprimer un domaine alias.
3. Naviguez vers **Paramètres client** > **Domaines**.

4. Cliquez sur la flèche du menu à côté de l'alias de domaine que vous souhaitez supprimer.

Un menu s'ouvre.

5. **PRUDENCE :**

Dès que le domaine alias est supprimé, toutes les adresses courriel associées ainsi que les paramètres du domaine alias sont irrévocablement supprimés.

Si une adresse courriel du domaine supprimé était l'adresse principale d'une boîte aux lettres à laquelle une adresse courriel d'un autre domaine est attribuée comme adresse alias, l'adresse alias devient la nouvelle adresse principale de la boîte aux lettres. Si plusieurs adresses alias sont attribués à la boîte aux lettres, la première adresse alias créée devient l'adresse principale et les autres adresses alias restent les mêmes. À l'avenir, l'utilisateur de la boîte aux lettres devra utiliser la nouvelle adresse principale comme nom d'utilisateur dans le Control Panel.

Cliquez sur **Supprimer domaine**.

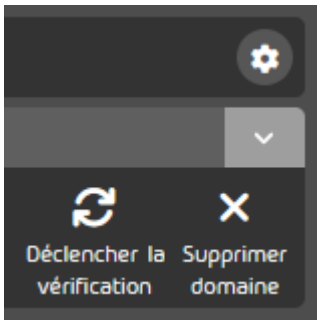


Illustration 223 : Supprimer le domaine

Un message d'avertissement apparaît.

6. Cliquez sur **Confirmer**.

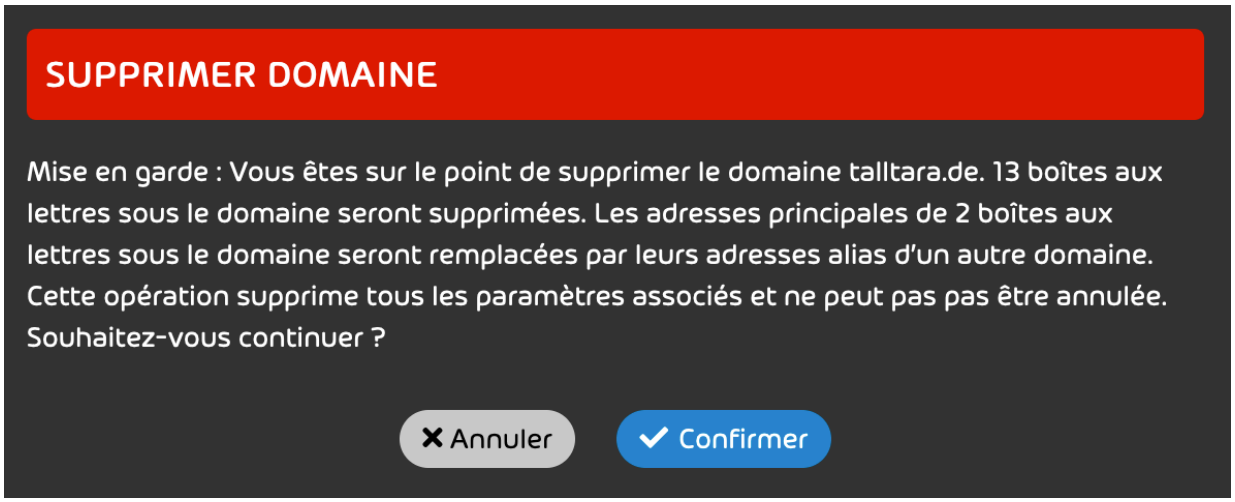


Illustration 224 : Confirmer la suppression

Le domaine alias, ses boîtes aux lettres et les paramètres du domaine alias sont supprimés du Control Panel. Le domaine alias est supprimé de la liste de domaines.

Un domaine alias a été supprimé du Control Panel.

Vérifications de domaines

Pour des raisons de sécurité, nous vérifions si un client est autorisé à gérer les domaines enregistrés dans le Control Panel. Nous vérifions donc les domaines enregistrés pour un client dans le module **Paramètres client** > **Domaines** (voir Domaines à la page 285).

REMARQUE :

Les administrateurs côté clients peuvent accéder à ce module s'ils sélectionnent le domaine principal du client dans la sélection de l'espace (voir Sélection de l'espace à la page 53).

Si un domaine réussit la vérification, celui-ci est vérifié. Le statut de la vérification est affiché par un symbole dans la colonne **Vérifié** dans le module **Paramètres client** > **Domaines**. Un domaine ne peut être vérifié que pour un seul client dans le Control Panel.

Tableau 19 : Vérifications de domaines

SYMBOLE	EXPLICATION
	Le domaine est vérifié.
	Le domaine n'est pas vérifié.

Nous vérifions un domaine pour la première fois pendant quelques minutes après qu'il a été ajouté au Control Panel. Nous déterminons alors si les entrées MX du domaine renvoient vers nous (voir « Migration des enregistrements MX »« Première configuration des services » dans les instructionsPremière configuration des services). Pour les domaines non vérifiés, la vérification est répétée toutes les heures. Les administrateurs côté client mais peuvent à tout moment démarrer manuellement la vérification d'un domaine non vérifié (voir Lancer la vérification à la page 296).

REMARQUE :

Si des problèmes surviennent lors de la vérification d'un domaine, le client peut contacter l'assistance ou son interlocuteur.

La vérification des domaines a des effets sur le module **Email Live Tracking** (voir Email Live Tracking à la page 59). En effet, seuls les courriels destinés aux boîtes aux lettres de domaines vérifiés sont affichés dans le module. Le domaine de la boîte aux lettres est indiqué pour chaque courriel dans le champ **Domaine du propriétaire** des détails du courriel (voir Informations élargies des courriels à la page 79). Dès qu'un domaine est vérifié, tous les courriels pour les boîtes aux lettres du domaine qui ont été envoyés à notre infrastructure apparaissent dans le module **Email Live Tracking**.

REMARQUE :

Les anciens courriels pour lesquels le champ **Domaine du propriétaire** est vide apparaissent également dans le module **Email Live Tracking**.

Les courriels de la catégorie **Refusé** sont également affichés dans le module. Cela permet d'éviter de perdre les courriels qui ont été envoyés à notre infrastructure avant la création du domaine dans le Control Panel et que nous avons donc refusés.

Lancer la vérification

Pour les domaines non vérifiés dans le module **Paramètres client** > **Domaines**, le système vérifie automatiquement une fois par jour si les domaines peuvent être vérifiés (voir Vérifications de domaines à la page 294). En outre, vous pouvez à tout moment lancer manuellement la vérification d'un domaine non vérifié.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine principal du client pour lequel vous souhaitez vérifier un domaine.
3. Naviguez vers **Paramètres client** > **Domaines**.
4. Cliquez sur la flèche de menu à côté du domaine non vérifié pour lequel vous souhaitez lancer un audit.

Illustration 225 : Ouvrir le menu

Un menu s'ouvre.

5. Cliquez sur **Déclencher la vérification**.

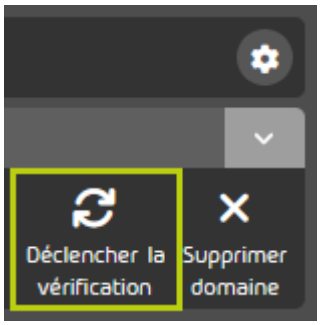


Illustration 226 : Démarrer la vérification

Nous vérifions si les enregistrements MX du domaine renvoient vers nous. Si le domaine passe la vérification, le statut du domaine dans la colonne **Vérifié** passe à **Vérifié**.

La vérification d'un domaine non vérifié a été lancée.

Authentification

Le module **Paramètres client** > **Authentification** permet aux administrateurs de définir des paramètres pour la connexion au Control Panel.

Les administrateurs côté clients et côté partenaires peuvent définir une politique de mot de passe pour les comptes des utilisateurs dans le Control Panel (voir Définir la longueur du mot de passe à la page 299). S'ils le souhaitent, les administrateurs peuvent réinitialiser les politique de mot de passe aux paramètres par défaut (voir Réinitialiser la longueur de mot de passe à la page 300).

REMARQUE :

Les politiques de mot de passe ne s'appliquent qu'aux mots de passe qui sont gérés dans le Control Panel (voir Types de boîtes aux lettres à la page 218).

Pour les boîtes aux lettres LDAP, les administrateurs côté clients peuvent définir si les identifiants des utilisateurs du service d'annuaire sont utilisées pour la connexion au Control Panel (voir Configurer une connexion dans le Control Panel via LDAP à la page 135) ou si les mots de passe des utilisateurs sont gérés dans le Control Panel.

Les administrateurs côté clients peuvent activer l'authentification multifacteur pour les utilisateurs d'un client (voir Activer l'authentification multifacteur à la page 301). Cela permet aux utilisateurs de configurer l'authentification multifacteur pour leur compte (voir le chapitre « Configurer l'authentification multifacteur » dans le manuel du Control Panel). L'authentification multifacteur améliore la sécurité lors de la connexion au Control Panel, car un mot de passe unique provenant d'une application Authenticator est nécessaire en plus du mot de passe du Control Panel. Il est également possible de forcer à nouveau l'authentification multifacteur pour les administrateurs (voir Forcer l'authentification multifacteur pour les administrateurs à la page 302). Les administrateurs peuvent également désactiver à nouveau l'authentification multifacteur pour les utilisateurs d'un client (voir Désactiver l'authentification multifacteur à la page 304).

REMARQUE :

Seuls les utilisateurs dont les mots de passe sont gérés dans le Control Panel ou dans un service d'annuaire via LDAP peuvent configurer l'authentification multifacteur dans le Control Panel.

Pour des raisons de sécurité, les utilisateurs inactifs seront automatiquement déconnectés du Control Panel au bout de 24 heures par défaut. Les administrateurs côté clients peuvent définir un délai plus court avant la déconnexion automatique ou désactiver la déconnexion automatique pour les utilisateurs d'un client (voir Configurer la déconnexion automatique à la page 306). S'ils le souhaitent, les administrateurs côté clients peuvent réinitialiser ultérieurement les paramètres par défaut (voir Réinitialiser les paramètres par défaut de la déconnexion automatique à la page 308).

Par défaut, il est possible de se connecter au Control Panel à partir de n'importe quelle adresse IPv4. Pour améliorer la sécurité, les administrateurs côté partenaires et côté clients peuvent toutefois définir que leurs utilisateurs ne peuvent accéder au Control Panel qu'à partir d'adresses IPv4 spécifiques ou de plages d'adresses IPv4 spécifiques. Les administrateurs peuvent limiter la connexion à des adresses IPv4 ou plages d'adresses IPv4 spécifiques en ajoutant ces adresses IPv4 ou plages d'adresses IPv4 au module **Paramètres client** > **Authentification** (voir Attribuer une adresse IP à la page 310). Les administrateurs peuvent également à nouveau supprimer des adresses IPv4 et des plages d'adresses IPv4 du module (voir Supprimer une adresse IP à la page 310). Si aucune adresse IPv4 et aucune plage d'adresses IPv4 ne sont disponibles dans le

module, la connexion sera possible à partir de n'importe quelle adresse IPv4. Si ce n'est pas le cas, la connexion sera limitée aux adresses IPv4 et aux plages d'adresses IPv4 existantes.

Définir la longueur du mot de passe

Vous pouvez également consulter d'autres exigences minimales pour les nouveaux mots de passe, qui sont définies par le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine, pour lequel vous souhaitez définir des politiques de mots de passe.
3. Naviguez vers **Paramètres client** > **Authentification**.

   IMPORTANT :

   La politique de mot de passe est transmise par les partenaires de niveau supérieur aux clients de niveau inférieur. Les clients subordonnés peuvent renforcer la politique de mot de passe, mais pas l'affaiblir. Par exemple, les clients subordonnés peuvent augmenter la longueur du mot de passe, mais pas la raccourcir.

4. Saisissez la longueur minimale du mot de passe dans le champ de saisie **Longueur du mot de passe**.

   REMARQUE :

   La longueur minimale du mot de passe doit être d'au moins 8 caractères.

   REMARQUE :

   D'autres exigences minimales pour les nouveaux mots de passe sont affichées. Celles-ci sont prédéfinies par le Control Panel et ne peuvent pas être modifiées. Part conséquent, les nouveaux mots de passe doivent contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

5. Cliquez sur **Enregistrer** pour appliquer les paramètres.

La longueur minimale du mot de passe est mise à jour dans le Control Panel.

> **REMARQUE :**
>
> La nouvelle longueur minimale du mot de passe n'est obligatoire que pour les nouveaux mots de passe créés et n'a aucun effet sur les mots de passe existants.

La longueur minimale du mot de passe a été définie pour un domaine.

Les politiques de mots de passe peuvent ensuite être réinitialisées (voir Réinitialiser la longueur de mot de passe à la page 300).

Réinitialiser la longueur de mot de passe

Vous avez défini une longueur minimale de mot de passe pour un domaine (voir Définir la longueur du mot de passe à la page 299).

Le module **Paramètres client** > **Authentification** vous permet de réinitialiser la longueur minimale définie du mot de passe pour un domaine aux paramètres par défaut. Les paramètres par défaut sont ceux qui ont été spécifiés par les administrateurs supérieurs.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine vous souhaitez réinitialiser la longueur minimale de mot de passe.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Cliquez sur **Paramètres par défaut** pour réinitialiser la longueur minimale de mot de passe aux parammètres par défaut.
5. Cliquez sur **Enregistrer** pour appliquer les paramètres.

La longueur minimale de mot de passe pour un domaine a été réinitialisée aux paramètres par défaut.

Activer l’ authentification multifacteur

Vous pouvez activer l'authentification multifacteur pour les utilisateurs d'un domaine. Cela permet aux utilisateurs du domaine de configurer l'authentification multifacteur pour leur compte dans le Control Panel (voir le chapitre « Configurer l'authentification multifacteur » dans le manuel du Control Panel).

REMARQUE :

Seuls les utilisateurs dont les mots de passe sont gérés dans le Control Panel ou dans un service d'annuaire via LDAP peuvent configurer l'authentification multifacteur dans le Control Panel.

L'authentification multifacteur améliore la sécurité lors de la connexion au Control Panel, car un mot de passe unique provenant d'une application Authenticator est nécessaire en plus du mot de passe du Control Panel. Nous recommandons en particulier aux administrateurs de configurer l'authentification multifacteur pour leur compte.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer l'authentification multifacteur.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Actionnez le bouton **Autoriser les utilisateurs à utiliser l'authentification multifacteur** sous **Authentification multifacteur**.

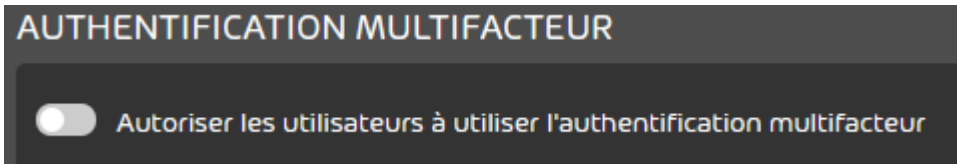


Illustration 227 : Activer l’ authentification multifacteur

- Le bouton devient vert et une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

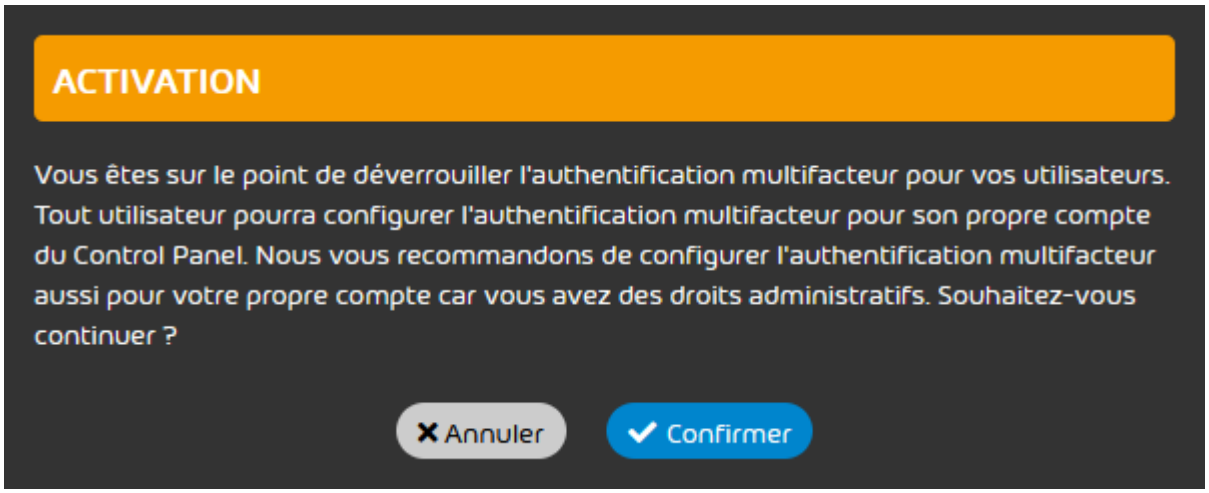


Illustration 228 : Confirmer

L'authentification multifacteur est activée pour les utilisateurs du domaine.

L'authentification multifacteur a été activée pour les utilisateurs d'un domaine.

Les utilisateurs du domaine peuvent ensuite configurer l'authentification multifacteur pour leur compte du Control Panel (voir le chapitre « Configurer l'authentification multifacteur » dans le manuel du Control Panel). Si un utilisateur rencontre des problèmes avec l'authentification multifacteur, vous pouvez réinitialiser l'authentification multifacteur de l'utilisateur (voir Réinitialiser l'authentification multifacteur à la page 261).

Forcer l'authentification multifacteur pour les administrateurs

Vous avez activé l'authentification multifacteur (voir Activer l'authentification multifacteur à la page 301).

Vous pouvez activer l'authentification multifacteur pour les administrateurs d'un client. Cela force tous les administrateurs du client à configurer l'authentification multifacteur pour leur compte dans le Control Panel (voir le chapitre « Configurer l'authentification multifacteur » dans le manuel du Control Panel).

REMARQUE :

Seuls les utilisateurs dont les mots de passe sont gérés dans le Control Panel ou dans un service d'annuaire via LDAP peuvent configurer l'authentification multifacteur dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour les administrateurs duquel vous souhaitez forcer l'authentification multifacteur.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Actionnez le bouton **Appliquer l'authentification multifacteur pour les administrateurs** sous **Authentification multifacteur**.

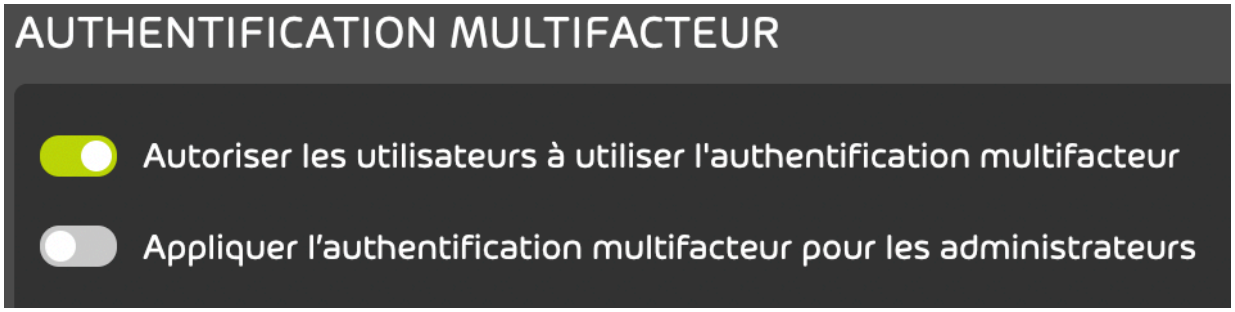


Illustration 229 : Forcer l'authentification multifacteur pour les administrateurs

Le bouton devient vert. Une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

Illustration 230 : Confirmer

L'authentification multifacteur est forcée pour tous les administrateurs du client.

L'authentification multifacteur a été forcée pour tous les administrateurs du client.

La prochaine fois que les administrateurs du client se connecteront au Control Panel, ils devront configurer l'authentification multifacteur pour leur compte du Control Panel (voir Configurer l'authentification multifacteur à partir de l'étape 7 à la page 27le chapitre « Configurer l'authentification multifacteur » à partir de l'étape 7 à la page 27 dans le manuel du Control Panel).

Désactiver l'authentification multifacteur

Vous avez activé l'authentification multifacteur pour les utilisateurs d'un domaine (voir Activer l'authentification multifacteur à la page 301).

Vous pouvez désactiver l'authentification multifacteur pour les utilisateurs d'un domaine. Les utilisateurs ne sont alors plus autorisés à configurer l'authentification multifacteur pour leur compte de Control Panel. La configuration est annulée pour les utilisateurs qui avaient déjà configuré l'authentification multifacteur.

REMARQUE :

Seuls les utilisateurs dont les mots de passe sont gérés dans le Control Panel ou dans un service d'annuaire via LDAP peuvent configurer l'authentification multifacteur dans le Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour les utilisateurs duquel vous souhaitez désactiver l'authentification multifacteur.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Actionnez le bouton **Autoriser les utilisateurs à utiliser l'authentification multifacteur** sous **Authentification multifacteur**.

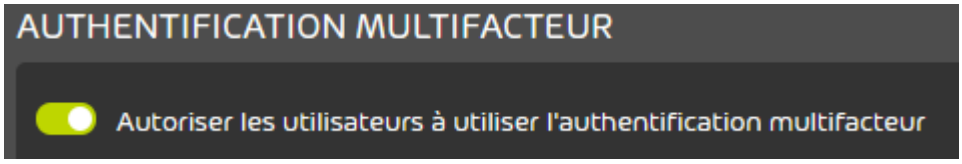


Illustration 231 : Désactiver l' authentification multifacteur

Le bouton devient gris et une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

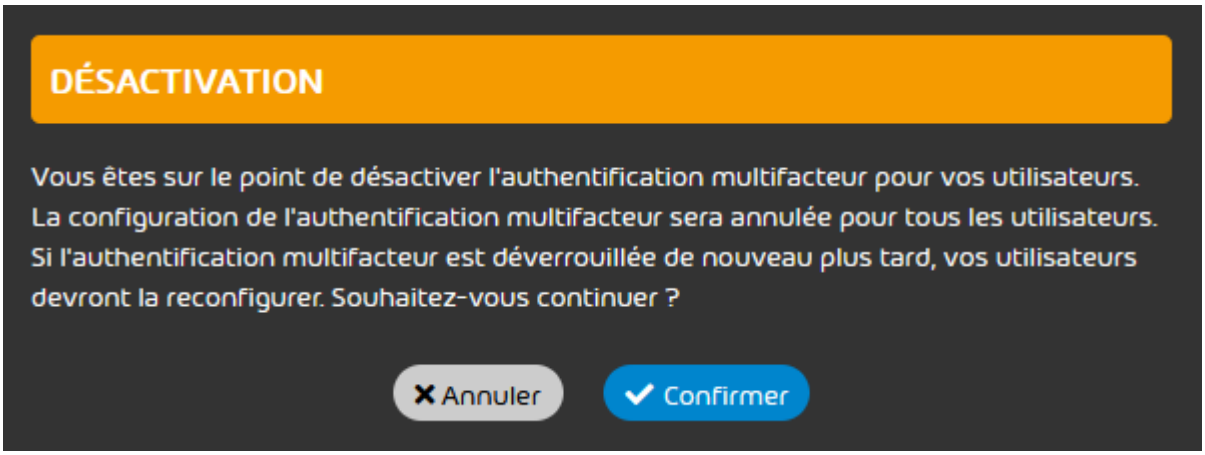


Illustration 232 : Confirmer

L'authentification multifacteur est désactivée pour les utilisateurs du domaine. La configuration est annulée pour les utilisateurs qui avaient déjà configuré l'authentification multifacteur. Les utilisateurs ne doivent désormais plus saisir que leur mot de passe de Control Panel lorsqu'ils se connectent au Control Panel.

> **REMARQUE :**
>
> Si l'authentification multifacteur est à nouveau activée par la suite pour les utilisateurs du domaine (voir Activer l' authentification multifacteur à la page 301), les utilisateurs peuvent reconfigurer l'authentification multifacteur (voir le chapitre «#Configurer l'authentification multifacteur#» dans le manuel du Control Panel).

L'authentification multifacteur a été désactivée pour les utilisateurs d'un domaine.

Configurer la déconnexion automatique

Pour des raisons de sécurité, les utilisateurs inactifs sont automatiquement déconnectés du Control Panel.

REMARQUE :

Par défaut, les utilisateurs inactifs sont automatiquement déconnectés du Control Panel au bout de 24 heures.

Le module **Paramètres client** > **Authentification** (voir Authentification à la page 297) vous permet de définir un délai plus court pour la déconnexion automatique ou de désactiver la déconnexion automatique pour les utilisateurs d'un client.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez modifier les paramètres de déconnexion automatique.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Si vous souhaitez définir un délai plus court avant la déconnexion automatique, réglez le délai souhaité dans les champs **heures** et **minutes** sous **Déconnexion automatique**.

   REMARQUE :

   Le délai de déconnexion automatique ne doit pas dépasser 24 heures.

Illustration 233 : Régler le delai

5. Si vous souhaitez désactiver la déconnexion automatique, décochez la case **Temps avant la déconnexion** sous **Déconnexion automatique**.

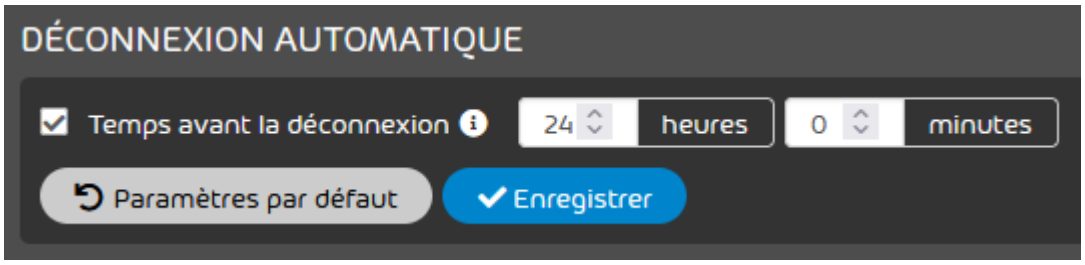


Illustration 234 : Désactiver la déconnexion automatique

La case n'est plus cochée et les paramètres de délai sont grisés.

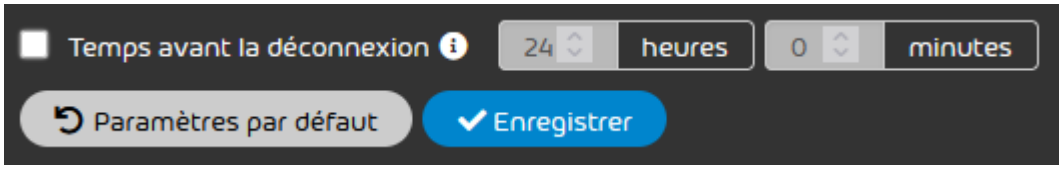


Illustration 235 : Aucune déconnexion automatique

6. Cliquez sur **Enregistrer**.

Les paramètres sont mémorisés. Un message de réussite apparaît.

Les paramètres de déconnexion automatique des utilisateurs d'un client ont été modifiés.

Vous pouvez ensuite rétablir les paramètres par défaut de la déconnexion automatique (voir Réinitialiser les paramètres par défaut de la déconnexion automatique à la page 308).

Réinitialiser les paramètres par défaut de la déconnexion automatique

Vous avez modifié les paramètres de déconnexion automatique des utilisateurs d'un client (voir Configurer la déconnexion automatique à la page 306).

Le module **Paramètres client** > **Authentification** (voir Authentification à la page 297) vous permet de rétablir les paramètres par défaut de déconnexion automatique des utilisateurs d'un client.

REMARQUE :

Par défaut, les utilisateurs inactifs sont automatiquement déconnectés du Control Panel au bout de 24 heures.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez rétablir les paramètres de déconnexion automatique par défaut.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Sous **Déconnexion automatique**, cliquez sur **Paramètres par défaut**.

Illustration 236 : Réinitialiser aux paramètres par défaut

Les paramètres par défaut de déconnexion automatique sont rétablis. Un message de réussite apparaît.

Illustration 237 : Paramètres par défaut

Les paramètres par défaut de déconnexion automatique des utilisateurs d'un client ont été rétablis.

Attribuer une adresse IP

Dans le module **Paramètres client** > **Authentification** vous pouvez autoriser pour un domaine la connexion au Control Panel uniquement à partir des adresses IP ou des plages d'adresses IP sélectionnées.

REMARQUE :

Si aucune IP n'est attribuée, toutes les adresses IP sont autorisées pour la connexion au Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine souhaité.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Sous **IP autorisées pour la connexion au Control Panel**, cliquez sur **Ajouter restriction**.
5. Saisissez une adresse IPv4 ou une plage d'adresses IPv4 valide et cliquez sur **Ajouter**.

Pour un domaine, une adresse IP ou une plage d'adresses IP a été ajoutée pour la connexion au Control Panel.

Vous pouvez ensuite supprimer l'adresse IP saisie (voir Supprimer une adresse IP à la page 310).

Supprimer une adresse IP

Vous avez limité la connexion au Control Panel pour un domaine à certaines adresses IPv4 ou plages d'adresses IPv4 (voir Attribuer une adresse IP à la page 310).

Dans le module **Paramètres client** > **Authentification**, vous pouvez supprimer des adresses IP ou des plages d'adresses IP saisies pour un domaine afin qu'il ne soit plus possible de se connecter au Control Panel depuis l'adresse IP ou la plage d'adresses IP. La connexion au Control Panel n'est possible qu'à partir des adresses IP et des plages d'adresses IP inscrites.

REMARQUE :

Si aucune adresse IPv4 n'est attribuée, toutes les adresses IPv4 sont autorisées pour la connexion au Control Panel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine souhaité.
3. Naviguez vers **Paramètres client** > **Authentification**.
4. Dans la ligne de l'adresse IP ou de la plage d'adresses IP à supprimer, cliquez à droite sur la flèche de menu.
5. Cliquez sur **Supprimer** pour supprimer l'adresse IP ou la plage d'adresses IP.

Une adresse IP ou une plage d'adresses IP a été supprimée de la liste des adresses IP autorisées pour la connexion au Control Panel. Si la liste contient encore des entrées, il n'est plus possible de se connecter au Control Panel depuis l'adresse IP ou la plage d'adresses IP supprimée. Si la liste est vide, il est possible de se connecter au Control Panel depuis n'importe quelle adresse IP.

Expéditeurs interdits et autorisés

À propos des expéditeurs interdits et autorisés

Le module **Expéditeurs interdits et autorisés** contient la liste d'expéditeurs interdits et la liste d'expéditeurs autorisés d'un utilisateur ou d'un client. Chaque utilisateur dispose de sa propre blacklist et de sa propre whitelist, qu'il peut gérer lui-même. Les administrateurs côté clients peuvent également accéder aux blacklists et aux whitelists personnelles de leurs utilisateurs en sélectionnant les utilisateurs dans la sélection de l'espace. Les administrateurs côté clients peuvent également gérer une blacklist et une whitelist pour l'ensemble de leur domaine. Dans la liste d'expéditeurs interdits et la liste d'expéditeurs autorisés au niveau du domaine, les entrées des différents utilisateurs du domaine sont affichées, en plus des entrées qui s'appliquent à tous les utilisateurs du domaine. Les expéditeurs interdits et autorisés sont traités dans un ordre fixe (voir Traitement des entrées des expéditeurs interdits et autorisés à la page 355).

La liste d'expéditeurs interdits permet aux utilisateurs et aux administrateurs côté clients que certains courriels entrants d'un utilisateur ou de tous les utilisateurs d'un client soient considérés comme des spams par le filtre de spam. Les courriels de la catégorie **Spam** ne sont pas directement envoyés au destinataire, mais sont mis en quarantaine. S'ils le souhaitent, les destinataires peuvent se faire envoyer des courriels de la catégorie **Spam** via le module **Email Live Tracking** ou via des rapports de quarantaine.

REMARQUE :

Dans le module **Email Live Tracking** (voir le chapitre « Email Live Tracking » dans le manuel du Control Panel), les courriels dont l'expéditeur figure sur la blacklist sont également affichés.

L'affichage ou non des courriels d'expéditeurs interdits dans les rapports de quarantaine (voir le chapitre « À propos du Quarantine Report » dans le manuel du Control Panel) dépend des paramètres des rapports de quarantaine. Les utilisateurs peuvent voir dans leurs paramètres utilisateur si les courriels des expéditeurs interdits sont exclus de leurs rapports de quarantaine (voir le chapitre « Configurer les rapports de quarantaine » dans le manuel du Control Panel). Si l'administrateur l'autorise, les utilisateurs peuvent modifier ce paramètre eux-mêmes.

La liste d'expéditeurs autorisés permet aux utilisateurs et aux administrateurs côté clients de contourner le filtre spam et/ou d'autres filtres pour certains courriels entrants d'un utilisateur ou de tous les utilisateurs d'un domaine.

IMPORTANT :

Grâce à la liste d'expéditeurs autorisés au niveau d'un utilisateur, les courriels ne font que contourner le filtre de spam. Si un expéditeur figure sur la liste d'expéditeurs autorisés, ses courriels, qui auraient normalement été catégorisés comme **Spam**, seront transmis au destinataire en tant que **Valide**. Si un courriel d'un expéditeur doit être classé sur la liste d'expéditeurs autorisés comme **Contenu**, **Threat**, **AdvThreat** ou **Refusé**, celui-ci n'est toutefois pas transmis.

Pour les entrées d'expéditeurs autorisés au niveau d'un domaine en revanche, les administrateurs côté clients peuvent sélectionner les filtres qui seront contournés par une entrée d'expéditeurs autorisés. D'autres filtres sont disponibles en plus du filtre de spam (voir Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). Les administrateurs côté clients peuvent, au niveau d'un domaine, aussi bien créer des entrées d'expéditeurs autorisés pour l'ensemble d'un domaine que des entrées d'expéditeurs autorisés pour les différents utilisateurs d'un client.

Les utilisateurs et les administrateurs côté clients peuvent créer des entrées d'expéditeurs interdits et d'expéditeurs autorisés directement dans le module **Expéditeurs interdits et autorisés** (voir Créer une entrée d'expéditeur interdit pour un utilisateur à la page 315 et Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317 pour la création d'entrées pour un utilisateur et Créer une entrée d'expéditeur interdit pour un domaine à la page 320 et Créer une entrée d'expéditeur autorisé pour un domaine à la page 322 pour la création d'entrées pour tous les utilisateurs d'un domaine). Les utilisateurs et les administrateurs côté clients peuvent également importer des entrées d'expéditeurs interdits et d'expéditeurs autorisés à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329). Les fichiers CSV doivent avoir une certaine structure. Les fichiers CSV qui permettent d'importer des entrées d'expéditeurs interdits et d'expéditeurs autorisés au niveau d'un utilisateur ou des entrées d'expéditeurs interdits au niveau d'un domaine sont soumis à une structure différente (voir Fichiers CSV pour importer des expéditeurs interdits et autorisés à la page 333) de celle des fichiers CSV qui permettent d'importer des entrées d'expéditeurs autorisés au niveau d'un domaine (voir Fichiers CSV pour l'importation d'entrées d'expéditeurs autorisés pour un domaine à la page 333).

REMARQUE :

L'importation CSV au niveau d'un domaine permet aux administrateurs côté clients d'importer également des entrées d'expéditeurs autorisés pour différents utilisateurs en plus des entrées d'expéditeurs autorisés pour un domaine (voir Fichiers CSV pour l'importation d'entrées d'expéditeurs autorisés pour un domaine à la page 333). À ce niveau, il est également possible d'importer des entrées d'expéditeurs autorisés pour des différents utilisateurs, qui contournent les filtres autres que le filtre de spam (voir Fichiers CSV pour l'importation d'entrées d'expéditeurs autorisés pour un domaine à la page 333).

Pour simplifier la gestion des entrées d'expéditeurs interdits et d'expéditeurs autorisés, les utilisateurs et les administrateurs côté clients peuvent exporter les entrées d'expéditeurs interdits et d'expéditeurs autorisés sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Il est également possible de rechercher dans les entrées de la blacklist et de la whitelist dans le Control Panel (voir Parcourir les entrées des expéditeurs interdits et autorisés à la page 354). Les entrées qui ne

sont plus nécessaires peuvent être supprimées (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Créer une entrée d'expéditeur interdit pour un utilisateur

Le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312) vous permet de placer des adresses courriel, des domaines ou des adresses IPv4 sur votre liste d'expéditeurs interdits ou sur la liste d'expéditeurs interdits d'un utilisateur de votre domaine. Les courriels entrants de l'utilisateur, qui proviennent de ces adresses courriel, domaines et adresses IP, sont considérés comme des spams par le filtre de spam.

REMARQUE :

Les administrateurs côté clients peuvent également créer des entrées d'expéditeurs interdits pour tous les utilisateurs de leur domaine (voir Créer une entrée d'expéditeur interdit pour un domaine à la page 320).

REMARQUE :

Au lieu de créer des entrées d'expéditeurs interdits une par une, les utilisateurs et les administrateurs côté clients peuvent également importer une liste d'entrées d'expéditeurs interdits à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Si vous souhaitez créer une entrée pour les expéditeurs interdits d'un utilisateur de votre domaine au lieu de vos propres expéditeurs interdits, sélectionnez l'utilisateur dans la sélection de l'espace.

   REMARQUE :

   Si aucun domaine n'est sélectionné dans la sélection de l'espace, l'utilisateur connecté est sélectionné.

3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs interdits**.
5. Cliquez sur **Ajouter entrée**.

Un affichage étendu s'ouvre.

Illustration 238 : Vue élargie

6. Dans le champ de gauche, saisissez l'adresse courriel, le domaine ou l'adresse IPv4 dont les courriels doivent être considérés comme des spams par le filtre de spam.

> **REMARQUE :**
>
> Pour les domaines, la syntaxe **nomdudomaine.tld** s'applique.

7. Facultatif : Dans le champ **Description**, saisissez une description de l'entrée d'expéditeur interdit.

> **REMARQUE :**
>
> Cette description est limitée à 100 caractères.

8. Cliquez sur **Ajouter**.

> **IMPORTANT :**
>
> Si l'entrée ajoutée se trouvait déjà sur la liste opposée, elle sera supprimée de cette dernière et ajoutée à cette liste.

L'entrée est créée et ajoutée au tableau des entrées d'expéditeurs interdits de l'utilisateur.

REMARQUE :

L'entrée d'expéditeur interdit est également affichée dans la liste d'expéditeurs interdits du domaine de l'utilisateur.

Une entrée d'expéditeur interdit a été créée pour un utilisateur.

Vous pouvez ensuite exporter les entrées d'expéditeurs interdits sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Si vous n'avez plus besoin d'une entrée d'expéditeur interdit, vous pouvez la supprimer (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Créer une entrée d'expéditeur autorisé pour un utilisateur

Le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312) vous permet de définir des adresses courriel, des domaines ou des adresses IPv4 sur votre liste d'expéditeurs autorisés ou sur la liste d'expéditeurs autorisés d'un utilisateur de votre domaine. Les courriels entrants de l'utilisateur qui proviennent de ces adresses courriel, domaines et adresses IPv4 contournent le filtre de spam.

REMARQUE :

Les administrateurs côté clients peuvent également créer des entrées d'expéditeurs autorisés pour tous les utilisateurs de leur domaine (voir Créer une entrée d'expéditeur interdit pour un domaine à la page 320).

IMPORTANT :

Grâce à la liste d'expéditeurs autorisés au niveau d'un utilisateur, les courriels ne font que contourner le filtre de spam. Si un expéditeur figure sur la liste d'expéditeurs autorisés, ses courriels, qui auraient normalement été catégorisés comme **Spam**, seront transmis au destinataire en tant que **Valide**. Si un courriel d'un expéditeur doit être classé sur la liste d'expéditeurs autorisés comme **Contenu**, **Threat**, **AdvThreat** ou **Refusé**, celui-ci n'est toutefois pas transmis.

Pour les entrées d'expéditeurs autorisés au niveau d'un domaine en revanche, les administrateurs côté clients peuvent sélectionner les filtres qui seront contournés par une entrée d'expéditeurs autorisés. D'autres filtres sont disponibles en plus du filtre de spam (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). Les administrateurs côté clients peuvent, au niveau d'un domaine, aussi bien créer des entrées d'expéditeurs autorisés pour l'ensemble d'un domaine que des entrées d'expéditeurs autorisés pour les différents utilisateurs d'un client.

REMARQUE :

Au lieu de créer des entrées d'expéditeurs autorisés une par une, les utilisateurs et les administrateurs côté clients peuvent également importer une liste d'entrées d'expéditeurs autorisés à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Si vous souhaitez créer une entrée pour la liste d'expéditeurs autorisés d'un utilisateur de votre domaine plutôt que pour votre propre liste d'expéditeurs autorisés, sélectionnez l'utilisateur dans la sélection de l'espace.

   REMARQUE :

   Si aucun domaine n'est sélectionné dans la sélection de l'espace, l'utilisateur connecté est sélectionné.

3. Naviguez vers **Expéditeurs interdits et autorisés**.

4. Sélectionnez l'onglet **Expéditeurs autorisés**.
5. Cliquez sur **Ajouter entrée**.

Un affichage étendu s'ouvre.

Illustration 239 : Vue élargie

6. Dans le champ de gauche, saisissez l'adresse courriel, le domaine ou l'adresse IPv4 dont les courriels ne doivent pas être marqués comme spam par le filtre de spam.

> **REMARQUE :**
>
> Pour les domaines, la syntaxe **nomdudomaine.tld** s'applique.

7. Facultatif : Dans le champ **Description**, saisissez une description de l'entrée d'expéditeur autorisé.

> **REMARQUE :**
>
> La description est limitée à 100 caractères.

8. Cliquez sur **Ajouter**.

> **IMPORTANT :**
>
> Si l'entrée ajoutée se trouvait déjà sur la liste opposée, elle sera supprimée de cette dernière et ajoutée à cette liste.

L'entrée est créée et ajoutée au tableau des entrées d'expéditeurs autorisés de l'utilisateur.

> **REMARQUE :**
>
> L'entrée d'expéditeur autorisé apparaît également dans la liste d'expéditeurs autorisés du domaine de l'utilisateur.

Vous pouvez ensuite exporter les entrées d'expéditeurs autorisés sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Si vous n'avez plus besoin d'une entrée d'expéditeur autorisé, vous pouvez la supprimer (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Créer une entrée d'expéditeur interdit pour un domaine

Dans le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312), vous pouvez placer des adresses courriel, des domaines ou des adresses IPv4 sur la liste des expéditeurs interdits de votre domaine. Les courriels entrants des utilisateurs de votre domaine qui proviennent de ces adresses courriel, domaines et adresses IP sont considérés comme des spams par le filtre de spam.

> **REMARQUE :**
>
> Au lieu de créer des entrées d'expéditeurs interdits individuellement, les administrateurs côté clients peuvent importer une liste d'entrées d'expéditeurs interdits à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une entrée d'expéditeur interdit.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs interdits**.

5. Cliquez sur **Ajouter entrée**.

Un affichage étendu s'ouvre.

Illustration 240 : Vue élargie

6. Dans le champ de gauche, saisissez l'adresse courriel, le domaine ou l'adresse IPv4 dont les courriels doivent être considérés comme des spams par le filtre de spam.

> **REMARQUE :**
>
> Pour les domaines, la syntaxe **nomdudomaine.tld** s'applique.

7. Facultatif : Dans le champ **Description**, saisissez une description de l'entrée d'expéditeur interdit.

> **REMARQUE :**
>
> Cette description est limitée à 100 caractères.

8. Cliquez sur **Ajouter**.

> **IMPORTANT :**
>
> Si l'entrée ajoutée se trouvait déjà sur la liste opposée, elle sera supprimée de cette dernière et ajoutée à cette liste.

L'entrée est créée et ajoutée au tableau des entrées d'expéditeurs interdits du domaine.

Une entrée d'expéditeur interdit a été créée pour un domaine.

Vous pouvez ensuite exporter les entrées d'expéditeurs interdits sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Si vous n'avez plus besoin d'une entrée d'expéditeur interdit, vous pouvez la supprimer (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Créer une entrée d'expéditeur autorisé pour un domaine

Le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312) vous permet de créer des entrées d'expéditeurs autorisés au niveau d'un domaine. Vous pouvez aussi bien créer des entrées d'expéditeurs autorisés pour votre domaine, qui s'appliquent à tous les utilisateurs du client, que des entrées pour des différents utilisateurs du client. Une entrée d'expéditeur autorisé détermine que certains courriels entrants contournent les filtres sélectionnés. Contrairement aux entrées d'expéditeurs autorisés créées au niveau d'un utilisateur (voir Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317), vous pouvez choisir, au niveau d'un domaine, quels filtres seront contournés par une entrée d'expéditeur autorisé.

REMARQUE :

Au lieu de créer des entrées d'expéditeurs autorisés individuellement, les administrateurs côté clients peuvent importer une liste d'entrées d'expéditeurs autorisés à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une entrée d'expéditeur autorisé.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs autorisés**.
5. Cliquez sur **Ajouter entrée**.

Un affichage étendu s'ouvre.

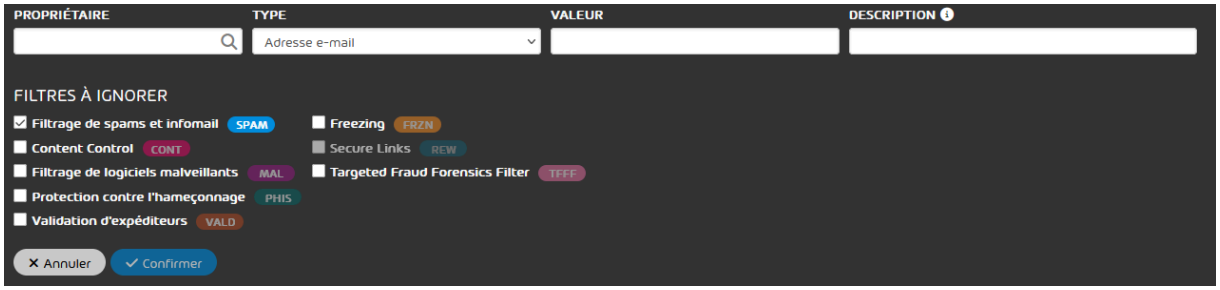


Illustration 241 : Vue élargie

6. **IMPORTANT :**

   Pour le Targeted Fraud Forensics Filter, le propriétaire n'est pas évalué. Les entrées d'expéditeurs autorisés qui contournent ce filtre s'appliquent toujours à tous les utilisateurs du client.

   Facultatif : Si l'entrée d'expéditeur autorisé ne doit s'appliquer qu'à un certain utilisateur du client, saisissez l'adresse courriel de cet utilisateur dans le champ **Propriétaire**. Pour déclencher la fonction de proposition automatique, entrez au moins trois caractères consécutifs.

   REMARQUE :

   Si le champ reste vide, l'entrée d'expéditeur autorisé s'applique au domaine du client. Dans ce cas, l'entrée d'expéditeur autorisé s'applique à tous les utilisateurs du client.

7. Dans le menu déroulant **Type**, sélectionnez l'information d'un courriel à laquelle l'entrée d'expéditeur autorisé doit se référer. Vous avez les options suivantes :

   - **Adresse e-mail** : L'entrée d'expéditeur autorisé s'applique aux courriels qui ont été envoyés depuis une adresse courriel spécifique.
   - **Domaine** : L'entrée d'expéditeur autorisé s'applique aux courriels qui ont été envoyés depuis une adresse courriel d'un domaine spécifique.
   - **Adresse ou plage IP** : L'entrée d'expéditeur autorisé s'applique aux courriels qui ont été envoyés depuis une adresse IPv4 ou une plage d'adresses IPv4 spécifique.
   - **Domaine du site web (uniquement pour Secure Links)** : Une entrée d'expéditeur autorisé de ce type permet de contourner uniquement le moteur Secure Links d'Advanced Threat Protection (voir le chapitre « Description des moteurs ATP » dans le manuel du Control Panel). Cette entrée d'expéditeur autorisé empêche que dans les courriels entrants, les liens qui renvoient à un site Web spécifique soient réécrits par le moteur Secure Links. L'entrée d'expéditeur autorisé peut également être étendue aux sous-domaines du domaine.

Si l'option **Domaine du site web (uniquement pour Secure Links)** a été sélectionnée, la case **Inclure les sous-domaines** s'affichera sous le champ **Valeur**. Pour cette option sous **Filtres à ignorer**, la case **Secure Links** est cochée et toutes les autres cases sont grisées. Si une autre option a été sélectionnée, la case **Filtrage de spams et infomails** est cochée.

8. Dans le champ **Valeur**, saisissez la valeur des courriels auxquels l'entrée d'expéditeur autorisé doit s'appliquer. En fonction de votre sélection à l'étape 7 à la page 324, saisissez l'une des valeurs suivantes :

   - **Adresse e-mail** : Adresse courriel de l'expéditeur
   - **Domaine** : Domaine de l'expéditeur
   - **Adresse ou plage IP** : Adresse IPv4 ou plage d'adresses IPv4 à partir de laquelle le courriel a été envoyé
   - **Domaine du site web (uniquement pour Secure Links)** : Domaine du site Web auquel renvoie un lien dans le courriel

Le bouton **Confirmer** est déverrouillé.

9. Facultatif : Si, à l'étape 7 à la page 324, vous avez choisi l'option **Domaine du site web (uniquement pour Secure Links)** et que l'entrée d'expéditeur autorisé doit également s'appliquer aux liens contenant un sous-domaine du domaine saisi à l'étape 8 à la page 324, cochez la case **Inclure les sous-domaines**.

Illustration 242 : Tenir compte des sous-domaines

10. Facultatif : Dans le champ **Description**, saisissez une description de l'entrée d'expéditeur autorisé.

> **REMARQUE :**
>
> La description est limitée à 100 caractères.

11. Sous **Filtres à ignorer**, cochez les cases des filtres qui doivent être contournés par l'entrée d'expéditeur autorisé pour un courriel. Vous avez les options suivantes :

- **Filtrage de spams et infomails** : Le filtre de spam et le filtre d'infomail Spam and Malware Protection sont contournés. L'entrée d'expéditeur autorisé empêche que les courriels ne

soient considérés comme des spams par le filtre de spam ou comme des infomails par le filtre d'infomail.

> **REMARQUE :**
>
> Ce filtre est le seul filtre sélectionné par défaut, à l'exception des entrées d'expéditeurs autorisés de type **Domaine du site web (uniquement pour Secure Links)**, ce qui correspond au réglage des entrées d'expéditeurs autorisés des utilisateurs (voir Créer une entrée d' expéditeur autorisé pour un utilisateur à la page 317).

- **Content Control** : Le filtre Content Control (voir le chapitre « À propos du Content Control » dans le manuel du Control Panel) de la Spam and Malware Protection est contourné. L'entrée d'expéditeur autorisé empêche que les courriels soient classés comme **Contenu**.
- **Filtrage de logiciels malveillants** : Le filtre de maliciels de la Spam and Malware Protection est contourné. L'entrée d'expéditeur autorisé empêche que les courriels contenant des maliciels soient classés comme **Threat**.
- **Protection contre l'hameçonnage** : La protection contre le hameçonnage de la Spam and Malware Protection est contournée. L'entrée d'expéditeur autorisé empêche que les courriels de hameçonnage soient classés comme **Threat**.
- **Validation d'expéditeurs** : La validation de l'expéditeur de la Spam and Malware Protection est contournée. L'entrée d'expéditeur autorisé empêche que les courriels dont la validation de l'expéditeur a échoué ne soient refusés par notre serveur de messagerie.
- **Freezing** : Le moteur Freezing (voir le chapitre « Description des moteurs ATP » dans le manuel du Control Panel) d'Advanced Threat Protection est contourné.
- **Secure Links** : Le moteur Secure Links (voir le chapitre « Description des moteurs ATP » dans le manuel du Control Panel) d'Advanced Threat Protection est contourné.

> **REMARQUE :**
>
> Le moteur Secure Links ne peut être contourné que pour les entrées d'expéditeurs autorisés de type **Domaine du site web (uniquement pour Secure Links)** (voir l'étape 7 à la page 324). Le moteur Secure Links ne s'applique pas aux liens du domaine saisi dans les courriels entrants du propriétaire (voir l'étape 8 à la page 324).

- **Targeted Fraud Forensics Filter** : Le moteur Targeted Fraud Forensics Filter (voir le chapitre « Description des moteurs ATP » dans le manuel du Control Panel) d'Advanced Threat Protection ne vérifie pas, pour certains courriels entrants provenant d'une adresse courriel externe, s'ils donnent l'impression d'avoir été envoyés au nom d'un utilisateur spécifique du Control Panel. Toutefois, le moteur Targeted Fraud Forensics Filter vérifie

comme d'habitude si ces courriels donnent l'impression d'avoir été envoyés au nom d'autres utilisateurs du Control Panel.

REMARQUE :

Dans l'exemple suivant, il peut être judicieux de contourner le moteur Targeted Fraud Forensics Filter pour un utilisateur : Un utilisateur du client communique régulièrement avec d'autres collaborateurs de l'entreprise via une autre adresse courriel (par ex. son adresse courriel privée) que celle sous laquelle l'utilisateur est présent dans le Control Panel. Pour que ces courriels ne soient pas catégorisés comme **AdvThreat**, l'administrateur du client peut créer une entrée d'expéditeur autorisé pour cette adresse courriel alternative et contourner le moteur Targeted Fraud Forensics Filter pour l'utilisateur correspondant dans le Control Panel.

REMARQUE :

Les filtres font partie des services. Si l'un de ces services n'est pas activé pour le client, le filtre correspondant peut aussi ne pas être activé pour le client. Dans ce cas, un triangle d'avertissement jaune apparaît derrière le filtre. Il n'y a alors aucun effet lorsque le filtre est contourné. Toutefois, il est possible de sélectionner le filtre.

12. Si vous avez sélectionné l'option **Targeted Fraud Forensics Filter**, saisissez dans le champ **Utilisateur correspondant du Control Panel** l'adresse courriel de l'utilisateur pour laquelle le moteur Targeted Fraud Forensics Filter doit être contourné.
13. Cliquez sur **Confirmer**.

IMPORTANT :

Si l'entrée ajoutée se trouvait déjà sur la liste opposée, elle sera supprimée de cette dernière et ajoutée à cette liste.

L'entrée d'expéditeur autorisé est enregistrée et ajoutée au tableau des entrées d'expéditeurs autorisés.

Une entrée d'expéditeur autorisé a été créé au niveau d'un domaine.

Vous pouvez ensuite exporter les entrées d'expéditeurs autorisés sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Si vous n'avez plus besoin d'une entrée d'expéditeur autorisé, vous pouvez la supprimer (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV

Au lieu de créer des entrées d'expéditeurs interdits et d'expéditeurs autorisés individuellement pour un utilisateur (voir Créer une entrée d'expéditeur interdit pour un utilisateur à la page 315 et Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317) ou pour un domaine (voir Créer une entrée d'expéditeur interdit pour un domaine à la page 320 et Créer une entrée d'expéditeur autorisé pour un domaine à la page 322), le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312) vous permet de créer plusieurs entrées d'expéditeurs interdits et d'expéditeurs autorisés à partir d'un fichier CSV.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Si vous souhaitez importer des entrées pour la blacklist ou la whitelist de votre domaine ou d'un utilisateur du domaine, sélectionnez le domaine ou l'utilisateur dans la sélection de l'espace.

   REMARQUE :

   Si aucun domaine n'est sélectionné dans la sélection de l'espace, l'utilisateur connecté est sélectionné.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Si vous souhaitez importer les entrées des expéditeurs interdits, sélectionnez l'onglet **Expéditeurs interdits**. Si vous souhaitez importer les entrées des expéditeurs autorisés, sélectionnez l'onglet **Expéditeurs autorisés**.

5. Cliquez sur **Importer au format CSV**.

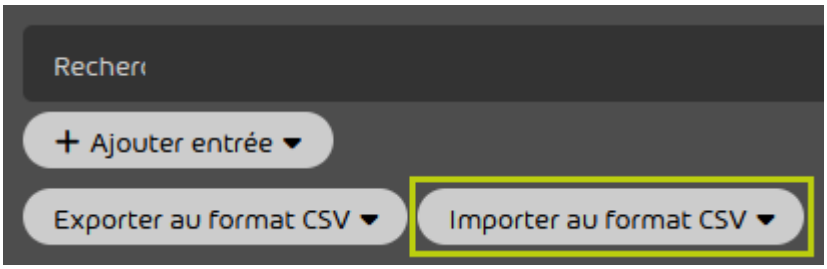


Illustration 243 : Importer un fichier CSV

- Un affichage étendu s'ouvre.

6. Cliquez sur **Charger fichier**.

Illustration 244 : Charger un fichier

7. **IMPORTANT :**

   Pour le fichier CSV, les consignes structurelles s'appliquent. L'importation d'entrées d'expéditeurs interdits et d'expéditeurs autorisés pour un utilisateur ainsi que l'importation d'entrées d'expéditeurs interdits pour un domaine (voir Fichiers CSV pour importer des expéditeurs interdits et autorisés à la page 333) sont soumises à d'autres consignes que celles pour l'importation d'entrées d'expéditeurs autorisés au niveau d'un domaine (voir Fichiers CSV pour l'importation d'entrées d'expéditeurs autorisés pour un domaine à la page 333).

   Sélectionnez le fichier CSV dans votre système de fichiers et cliquez sur **Ouvrir**.

- Il est indiqué le nombre d'entrées valides qui peuvent être importées depuis le fichier CSV.

REMARQUE :

Si une entrée ne peut pas être importée, un avertissement apparaît pour cette entrée.

Illustration 245 : Entrées à ajouter pour un utilisateur

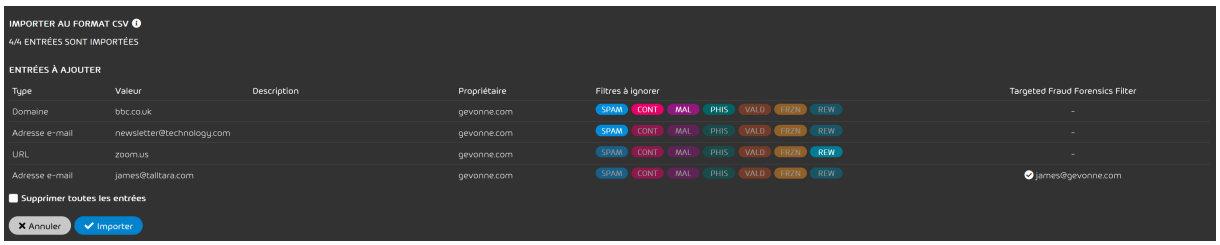


Illustration 246 : Entrées à ajouter aux expéditeurs autorisés d' un domaine

8. Facultatif : Si vous souhaitez supprimer toutes les entrées existantes des expéditeurs interdits ou autorisés dans le Control Panel, cliquez sur **Supprimer toutes les entrées**.

Une fois l'étape 9 à la page 332 effectuée, toutes les entrées existantes sont supprimées de la liste d'expéditeurs interdits ou d'expéditeurs autorisés et les entrées du fichier CSV sont importées dans la liste d'expéditeurs interdits ou d'expéditeurs autorisés.

9. Cliquez sur **Importer**.

Les entrées du fichier CSV sont importées dans la liste d'expéditeurs interdits ou la liste d'expéditeurs autorisés. Les entrées non valides et déjà existantes ne sont pas importées.

Illustration 247 : Entrées importées pour un utilisateur

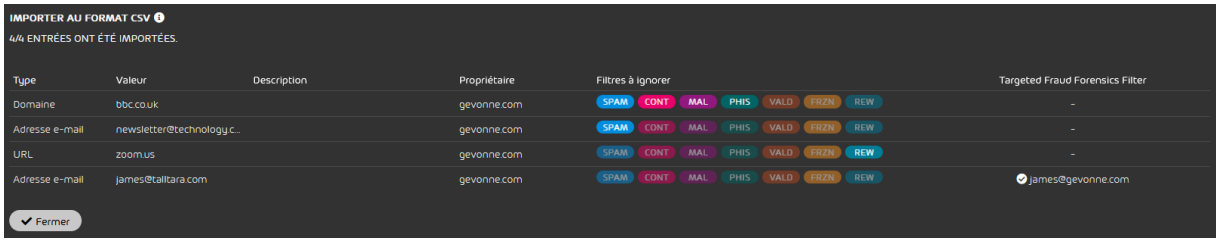


Illustration 248 : Entrées importées pour les expéditeurs autorisés d'un domaine

Des expéditeurs interdits ou autorisés ont été importés à partir d'un fichier CSV.

Vous pouvez ensuite exporter les entrées d'expéditeurs interdits ou d'expéditeurs autorisés sous forme de fichier CSV (voir Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV à la page 350). Si vous n'avez plus besoin d'une entrée, vous pouvez la supprimer (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

Fichiers CSV pour importer des expéditeurs interdits et autorisés

Des consignes structurelles s'appliquent aux fichiers CSV pour importer des expéditeurs interdits et autorisés (voir À propos des expéditeurs interdits et autorisés à la page 312). Le fichier d'importation doit remplir les conditions suivantes :

- L'extension du fichier à importer est .csv. Les autres extensions de fichier telles que .txt ou .docx ne seront pas acceptées.
- La première ligne contient la valeur du nom de la colonne **value**.
- Les lignes inférieures indiquent les domaines, les adresses courriel ou les adresses IPv4.
- Plusieurs entrées dans une ligne sont séparées par un point-virgule.

Fichiers CSV pour l'importation d'entrées d'expéditeurs autorisés pour un domaine

Les fichiers CSV servant à l'importation d'entrées d'expéditeurs autorisés (voir À propos des expéditeurs interdits et autorisés à la page 312) pour un domaine sont soumis à des exigences structurelles. Le fichier d'importation doit remplir les conditions suivantes.

Règles pour l'extension des fichiers

- L'extension du fichier à importer est .csv. D'autres extensions de fichier comme .txt ou .docx ne sont pas acceptées.

Règles pour les colonnes et les lignes

- Le fichier CSV contient 14 colonnes.
- Les colonnes sont séparées l'une de l'autre par un point-virgule.
- La première ligne contient les noms des colonnes (voir le tableau Tableau 20 : Colonnes à la page 334).
- À partir de la deuxième ligne, chaque ligne correspond à une entrée d'expéditeur autorisé.
- À partir de la deuxième ligne, chaque colonne contient une valeur (voir le tableau Tableau 20 : Colonnes à la page 334).

- Les lignes ne se terminent pas par des signes de ponctuation.

Tableau 20 : Colonnes

NUMÉRO	NOM DE LA COLONNE	VALEUR
1	value	Cette colonne peut contenir une adresse courriel, un domaine, une URL, une adresse IPv4 ou une plage d'adresses IPv4. La valeur correspond à la saisie dans le champ **Valeur** si une entrée d'expéditeur autorisé est créée manuellement (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). Le type de valeur qui doit être saisi dans cette colonne dépend du type d'entrée d'expéditeur autorisé, soit la valeur indiquée dans la colonne 4 **entry_type**. Pour de plus amples informations sur les entrées possibles, voir l'étape 8 à la page 324 au chapitre Créer une entrée d'expéditeur autorisé pour un domaine à la page 322.

NUMÉRO	NOM DE LA COLONNE	VALEUR
2	description	Cette colonne contient la description d'une entrée d'expéditeur autorisé. Cette valeur correspond à la saisie dans le champ **Description** si une entrée d'expéditeur autorisé est créée manuellement (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). La description doit comporter 100 caractères maximum. Cette description est facultative. La colonne peut donc être vide.

NUMÉRO	NOM DE LA COLONNE	VALEUR
3	owner	Cette colonne contient le propriétaire de l'entrée d'expéditeur autorisé. Si l'entrée d'expéditeur autorisé doit s'appliquer à tous les utilisateurs d'un client, la valeur est le domaine principal du client. Cependant, il est également possible de saisir un utilisateur du client comme propriétaire. Si l'entrée d'expéditeur autorisé doit s'appliquer à un utilisateur du client, la valeur est l'adresse courriel de l'utilisateur. **IMPORTANT :** Pour le Targeted Fraud Forensics Filter, le propriétaire n'est pas évalué. Les entrées d'expéditeurs autorisés qui contournent ce filtre s'appliquent toujours à tous les utilisateurs du client.

NUMÉRO	NOM DE LA COLONNE	VALEUR
4	entry_type	Cette colonne contient le type de l'entrée d'expéditeur autorisé. Sa valeur correspond au champ **Type** si une entrée d'expéditeur autorisé est créée manuellement (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). Les valeurs possibles sont les suivantes : • **EMAIL** : Cette valeur correspond à l'option **Adresse e-mail**. • **DOMAIN** : Cette valeur correspond à l'option **Domaine**. • **IP** : Cette valeur correspond à l'option **Adresse ou plage IP**. • **URL** : Cette valeur correspond à l'option **Domaine du site web (uniquement pour Secure Links)**. Pour de plus amples informations sur les options, voir l'étape 7 à la page 324 dans le chapitre Créer une entrée d'expéditeur autorisé pour un domaine à la page 322.

IMPORTANT :

Si cette colonne

NUMÉRO	NOM DE LA COLONNE	VALEUR
5	spam_protection	La valeur dans cette colonne indique si le filtre de spam doit être contourné par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le filtre de spam ne doit pas être contourné. La valeur **1** signifie que le filtre de spam doit être contourné. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
6	content_filter	La valeur dans cette colonne indique si le Content Control doit être contourné par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le Content Control ne doit pas être contourné. La valeur **1** signifie que le Content Control doit être contourné. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
7	malware_protection	La valeur dans cette colonne indique si le filtre de maliciels doit être contourné par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le filtre de maliciels ne doit pas être contourné. La valeur **1** signifie que le filtre de maliciels doit être contourné. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
8	phishing_protection	La valeur dans cette colonne indique si la protection contre le hameçonnage doit être contournée par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que la protection contre le hameçonnage ne doit pas être contournée. La valeur **1** signifie que la protection contre le hameçonnage doit être contournée. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
9	sender_validation	La valeur dans cette colonne indique si la validation de l'expéditeur doit être contournée par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que la validation de l'expéditeur ne doit pas être contournée. La valeur **1** signifie que la validation de l'expéditeur doit être contournée. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
10	email_freezing	La valeur dans cette colonne indique si le moteur Freezing d'Advanced Threat Protection doit être contourné par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le moteur Freezing ne doit pas être contourné. La valeur **1** signifie que le moteur Freezing doit être contourné. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
11	atp_url_rewriting	La valeur dans cette colonne indique si le moteur Secure Links d'Advanced Threat Protection doit être contourné par l'entrée d'expéditeur autorisé (voir l'étape 11 à la page 325 au chapitre Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le moteur Secure Links ne doit pas être contourné. La valeur **1** signifie que le moteur Secure Links doit être contourné. **IMPORTANT :** Si la colonne entry_type contient la valeur **URL**, cette colonne doit contenir la valeur **1**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
12	atp_tfff	La valeur dans cette colonne indique si le moteur Targeted Fraud Forensics Filter d'Advanced Threat Protection doit être contourné (voir l'étape 11 à la page 325 au chapitre Créer une entrée d' expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le moteur Targeted Fraud Forensics Filter ne doit pas être contourné. La valeur **1** signifie que le moteur Targeted Fraud Forensics Filter doit être contourné. **IMPORTANT :** Si la colonne 4 **entry_type** contient la valeur **URL**, ce filtre ne peut pas être contourné et la valeur dans cette colonne doit être **0**.

NUMÉRO	NOM DE LA COLONNE	VALEUR
13	atp_tfff_related_user	**IMPORTANT :** Cette colonne ne doit contenir qu'une seule valeur si le moteur Targeted Fraud Forensics Filter doit être contourné, c'est-à-dire si la colonne 12 **atp_tfff** contient la valeur **1**. Si ce n'est pas le cas, cette colonne doit être vide. La valeur dans cette colonne est l'adresse courriel de l'utilisateur du Control Panel pour lequel le moteur Targeted Fraud Forensics Filter doit être contourné. Cette valeur correspond à la saisie dans le champ **Utilisateur correspondant du Control Panel** si une entrée d'expéditeur autorisé est créée manuellement (voir Créer une entrée d' expéditeur autorisé pour un domaine à la page 322).

NUMÉRO	NOM DE LA COLONNE	VALEUR
14	atp_url_rewriting_include_subdomains	**IMPORTANT :** Cette colonne ne peut contenir la valeur **1** que si l'entrée d'expéditeur autorisé fait référence à une URL pour Secure Links, c'est-à-dire si la colonne **entry_type** contient la valeur **URL**. La valeur dans cette colonne indique si le moteur Secure Links doit également être contourné pour les URL avec un sous-domaine du domaine saisi dans la colonne 1 **value**. Cette colonne correspond au champ **Inclure les sous-domaines** si une entrée d'expéditeur autorisé est créée manuellement (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). La colonne peut contenir la valeur **0** ou **1**. La valeur **0** signifie que le moteur Secure Links ne doit pas être contourné pour les URL avec un sous-domaine. La valeur **1** signifie que le moteur Secure Links doit également être contourné pour les URL avec un sous-domaine.

Règle pour les doublons

- Les doublons n'ont aucune influence sur le traitement du fichier CSV.

Éditer une entrée d'expéditeur autorisé pour un domaine

Vous avez créé des entrées d'expéditeurs autorisés pour un domaine (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322) ou vous les avez importées à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

Dans le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312), vous pouvez éditer des entrées d'expéditeurs autorisés pour un domaine. Cela permet par exemple de modifier les filtres qui sont contournés par une entrée d'expéditeur autorisé.

REMARQUE :

Au niveau d'un domaine, les administrateurs côté clients peuvent également modifier les entrées d'expéditeurs autorisés existantes des utilisateurs de leur domaine. Les entrées d'expéditeurs autorisés créées au niveau de l'utilisateur (voir Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317) contournent le filtre de spam comme seul filtre. Au niveau d'un domaine, les administrateurs côté clients peuvent toutefois éditer les entrées d'expéditeurs autorisés des utilisateurs de façon à contourner les filtres autres que le filtre de spam. Indépendamment des filtres contournés, les entrées restent affichées au niveau des utilisateurs et peuvent être supprimées par ceux-ci (voir Supprimer une entrée d'expéditeur interdit ou autorisé à la page 352).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez éditer une entrée d'expéditeur autorisé.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs autorisés**.

5. Cliquez sur la flèche de menu à côté de l'entrée d'expéditeur autorisé que vous souhaitez éditer.

Illustration 249 : Ouvrir le menu

- Un menu s'ouvre.

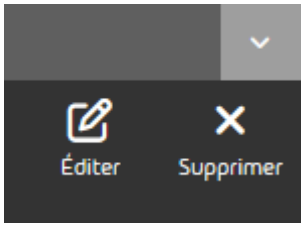


Illustration 250 : Menu

6. Cliquez sur **Éditer**.

- Un formulaire contenant les paramètres de l'entrée d'expéditeur autorisé s'ouvre.

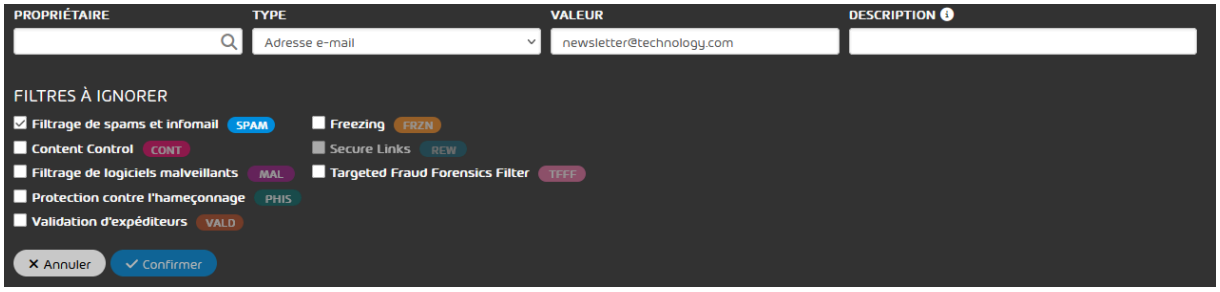


Illustration 251 : Paramètres de l'entrée d'expéditeur autorisé

7. Modifiez les paramètres en fonction de vos besoins (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322).

8. Cliquez sur **Confirmer**.

- Les modifications sont enregistrées.

Une entrée d'expéditeur autorisé a été éditée.

Exporter des entrées d'expéditeurs interdits ou d'expéditeurs autorisés en tant que fichier CSV

Vous avez créé des entrées d'expéditeurs interdits ou d'expéditeurs autorisés (voir Créer une entrée d'expéditeur interdit pour un utilisateur à la page 315 et Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317 pour la création d'entrées d'expéditeurs interdits ou d'expéditeurs autorisés pour un utilisateur et Créer une entrée d'expéditeur interdit pour un domaine à la page 320 et Créer une entrée d'expéditeur autorisé pour un domaine à la page 322 pour la création d'entrées d'expéditeurs interdits ou d'expéditeurs autorisés pour un domaine) ou les avez importé à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

Dans le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312), vous pouvez exporter toutes les entrées d'expéditeurs interdits et autorisés existantes sous forme de fichier CSV.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Si vous souhaitez exporter les entrées d'expéditeurs interdits ou d'expéditeurs autorisés de votre domaine ou d'un utilisateur du domaine au lieu de vos propres entrées, sélectionnez le domaine ou l'utilisateur dans la sélection de l'espace.

   REMARQUE :

   Si aucun domaine n'est sélectionné dans la sélection de l'espace, l'utilisateur connecté est sélectionné.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Si vous souhaitez exporter les entrées d'expéditeurs interdits, sélectionnez l'onglet **Expéditeurs interdits**. Si vous souhaitez exporter les entrées d'expéditeurs autorisés, sélectionnez l'onglet **Expéditeurs autorisés**.

5. Cliquez sur **Exporter au format CSV**.

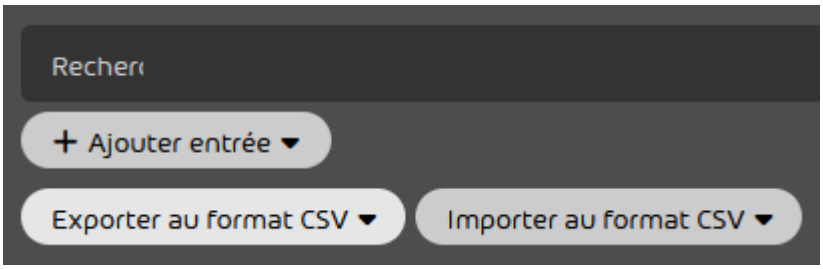


Illustration 252 : Exporter des entrées sous forme de fichier CSV

Les paramètres pour l'exportation CSV sont affichés.

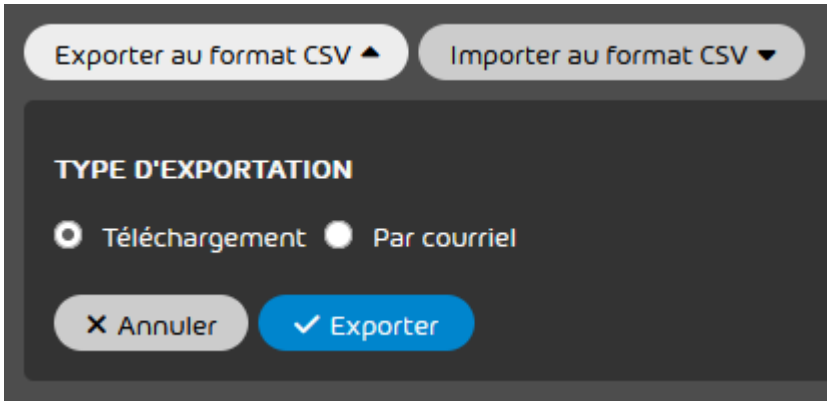


Illustration 253 : Paramètres pour l' exportation CSV

6. Sous **Type d'exportation**, indiquez si le fichier CSV doit être mis à disposition en téléchargement ou envoyé par courriel.
   - **Téléchargement** : le fichier CSV est mis à disposition dans les téléchargements.
   - **Par courriel** : le fichier CSV est envoyé par courriel.

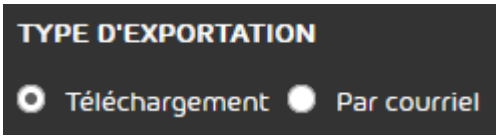


Illustration 254 : Sélectionner le type d'exportation

Si l'option **Par courriel** a été sélectionnée, un champ de saisie s'affiche.

7. Facultatif : Si vous avez sélectionné l'option **Par courriel**, saisissez l'adresse courriel à laquelle le fichier CSV doit être envoyé dans le champ de saisie.
8. Cliquez sur **Exporter**.

Les entrées des expéditeurs interdits ou des expéditeurs autorisés sont exportés sous forme de fichier CSV. Le fichier CSV est mis à disposition dans les téléchargements ou envoyé par courriel.

Les entrées des expéditeurs interdits ou des expéditeurs autorisés ont été exportés sous forme de fichier CSV.

Supprimer une entrée d'expéditeur interdit ou autorisé

Vous avez créé des entrées d'expéditeurs interdits ou d'expéditeurs autorisés (voir Créer une entrée d'expéditeur interdit pour un utilisateur à la page 315 et Créer une entrée d'expéditeur autorisé pour un utilisateur à la page 317 pour la création d'entrées d'expéditeurs interdits ou d'expéditeurs autorisés pour un utilisateur et Créer une entrée d'expéditeur interdit pour un domaine à la page 320 et Créer une entrée d'expéditeur autorisé pour un domaine à la page 322 pour la création d'entrées d'expéditeurs interdits ou d'expéditeurs autorisés pour un domaine) ou les avez importé à partir d'un fichier CSV (voir Importer des expéditeurs interdits et autorisés à partir d'un fichier CSV à la page 329).

Si vous n'avez plus besoin d'une entrée d'expéditeur interdit ou d'expéditeur autorisé, vous pouvez la supprimer dans le module **Expéditeurs interdits et autorisés** (voir À propos des expéditeurs interdits et autorisés à la page 312).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Si vous souhaitez supprimer un utilisateur autorisé ou un utilisateur interdit de votre domaine ou d'un utilisateur de votre domaine, sélectionnez le domaine ou l'utilisateur dans la sélection du domaine.

   REMARQUE :

   Si aucun domaine n'est sélectionné dans la sélection de l'espace, l'utilisateur connecté est sélectionné.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Si vous souhaitez supprimer une entrée d'expéditeur interdit, sélectionnez l'onglet **Expéditeurs interdits**. Si vous souhaitez supprimer une entrée d'expéditeur autorisé, sélectionnez l'onglet **Expéditeurs autorisés**.
5. Si vous souhaitez supprimer une entrée d'expéditeur interdit ou d'expéditeur autorisé d'un utilisateur ou une entrée d'expéditeur interdit d'un domaine, cliquez sur la croix à côté de l'entrée d'expéditeur interdit ou d'expéditeur autorisé. Si vous souhaitez supprimer une entrée d'expéditeur autorisé d'un domaine, cliquez sur la flèche de menu à côté de l'entrée d'expéditeur autorisé.

Illustration 255 : Supprimer une entrée d'expéditeur interdit ou d'expéditeur autorisé d'un utilisateur ou une entrée d'expéditeur interdit d'un domaine

Illustration 256 : Ouvrir le menu pour l'entrée d'expéditeur autorisé d'un domaine

- Si une entrée d'expéditeur interdit ou d'expéditeur autorisé d'un utilisateur ou une entrée d'expéditeur interdit d'un domaine a été sélectionnée, l'entrée d'expéditeur interdit ou

d'expéditeur autorisé sera supprimée. Si une entrée d'expéditeur autorisé d'un domaine a été sélectionnée, un menu s'ouvre.

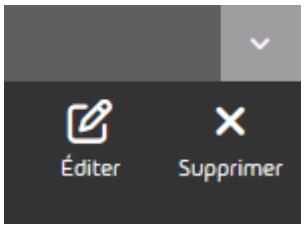


Illustration 257 : Menu pour l'entrée d'expéditeur autorisé d'un domaine

6. Si vous souhaitez supprimer une entrée d'expéditeur autorisé d'un domaine, cliquez sur **Supprimer**.

L'entrée d'expéditeur autorisé est supprimée.

Un expéditeur autorisé ou un expéditeur interdit a été supprimé.

Parcourir les entrées des expéditeurs interdits et autorisés

Dans le module **Blacklist & whitelist** (voir À propos des expéditeurs interdits et autorisés à la page 312), les entrées des expéditeurs interdits et autorisés peuvent être parcourues. Parcourir des entrées dans le module **Blacklist & whitelist** fonctionne comme dans le module **Email Live Tracking** (voir « Parcourir les courriels » dans le manuel du Control Panel).

Les termes de recherche peuvent être saisis dans la barre de recherche. Une terme de recherche peut être recherché soit dans tous les champs ou uniquement dans un des champs individuels **Valeur**, **Description** et **Propriétaire**. Les entrées sont filtrées dynamiquement.

En outre, les administrateurs côté clients peuvent parcourir les entrées d'expéditeurs autorisés pour les domaines selon les filtres contournés (voir Créer une entrée d'expéditeur autorisé pour un domaine à la page 322). Pour cela, des boutons colorés avec les noms des filtres contournés apparaissent en haut dans l'onglet **Expéditeurs autorisés**. Par défaut, tous ces boutons sont grisés et les entrées d'expéditeurs autorisés sont affichés pour tous les filtres. Pour n'afficher que les entrées d'expéditeurs autorisés qui contournent un ou plusieurs filtres spécifiques, les administrateurs côté clients peuvent cliquer sur les boutons de ces filtres et les activer pour le filtrage.

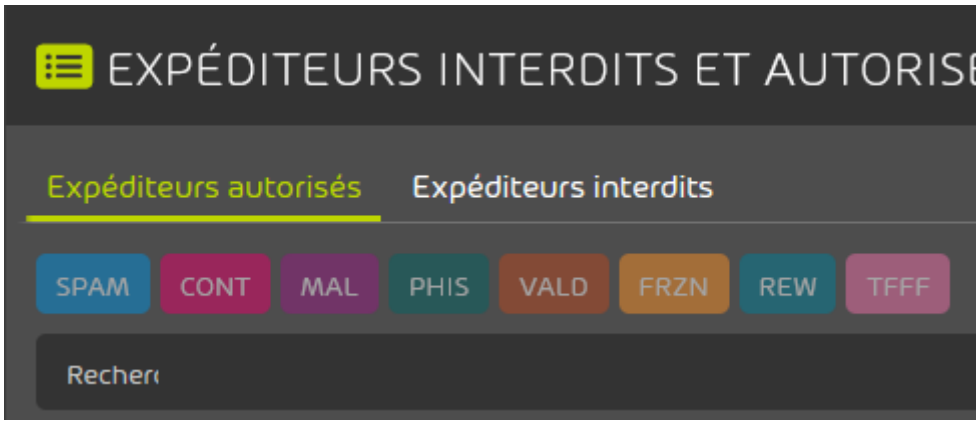


Illustration 258 : Boutons pour les filtres contournés dans les entrées d' expéditeurs autorisés

Exemple : Parcourir des entrées des expéditeurs interdits ou autorisés

Les expéditeurs interdits de l'utilisateur **klaus.trophobie@talltara.com** sont recherchés pour **domain**. Seuls les résultats qui commencent par **domain** sont affichés.

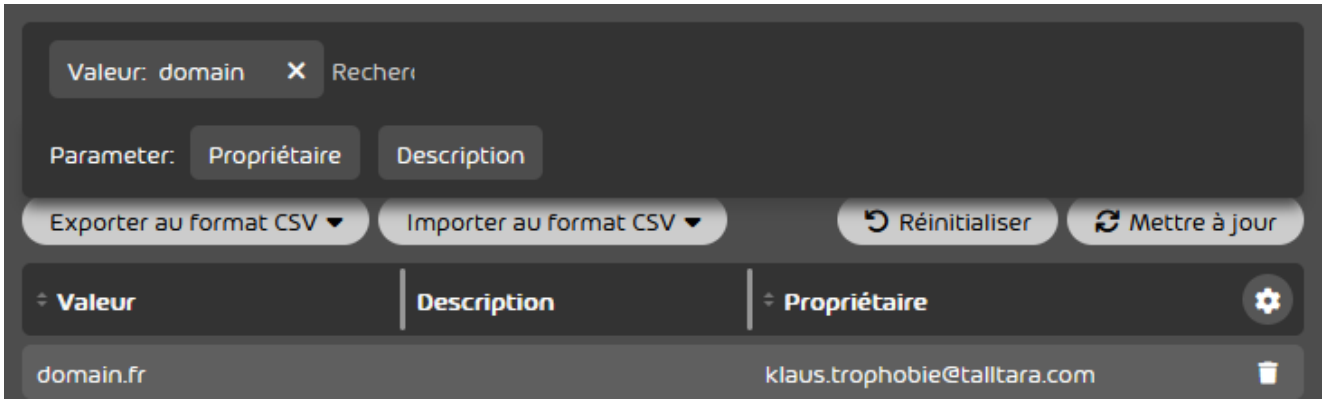


Illustration 259 : Parcourir les entrées des expéditeurs interdits et autorisés

Traitement des entrées des expéditeurs interdits et autorisés

Les entrées des expéditeurs interdits et autorisés (voir À propos des expéditeurs interdits et autorisés à la page 312) sont traitées comme suit de la priorité la plus élevée à la plus faible :

- Expéditeurs autorisés au niveau de l'utilisateur
- Expéditeurs interdits au niveau de l'utilisateur
- Expéditeurs autorisés au niveau du domaine et des groupes
- Expéditeurs interdits au niveau du domaine et des groupes

REMARQUE :

Il n'est plus possible de créer des entrées d'expéditeurs interdits/autorisés au niveau du partenaire ou des groupes. Toutefois, ces types d'entrées interdites et autorisées peuvent encore exister pour les clients existants.

Si une entrée appropriée a été trouvée dans l'une des listes, le traitement est arrêté et les listes suivantes ne sont pas prises en compte.

Exemple : Ordre de traitement des entrées de la blacklist et de la whitelist

Un administrateur interdit l'expéditeur **example@example.com** au niveau du domaine. Cependant, un utilisateur de ce domaine autorise cet expéditeur. Tous les courriels de l'expéditeur **example@example.com** seront envoyés à cet utilisateur, aucun courriel ne sera envoyé à tous les autres utilisateurs du domaine qui n'ont pas autorisé cet expéditeur eux-mêmes.

Paramètres de sécurité

Paramètres de sécurité

- Advanced Threat Protection
- Quarantine Report
- Spam and Malware Protection
- Content Control
- Compliance Filter
- Signature and Disclaimer
- Continuity Service

Advanced Threat Protection (ATP)

Structure et fonction d’ ATP

Advanced Threat Protection (ATP) protège les entreprises des attaques ciblées et individuelles.

Advanced Threat Protection (ATP) protège les entreprises des attaques ciblées et individuelles. Des moteurs d'analyse forensique innovants garantissent l'arrêt immédiat des attaques. En même temps, la solution fournit des informations détaillées sur les attaques contre l'entreprise.

L'ATP se compose des moteurs d'analyse suivants (voir Description des moteurs ATP à la page 360) :

- Moteur Sandbox
- Secure Links
- URL Scanning
- Freezing
- Targeted Fraud Forensics

Les courriels interceptés par l'ATP sont classés comme **AdvThreat** et mis en quarantaine et peuvent par défaut être distribués manuellement par les utilisateurs disposant de droits d'administration (voir le chapitre « Rôles » dans le manuel du Control Panel).

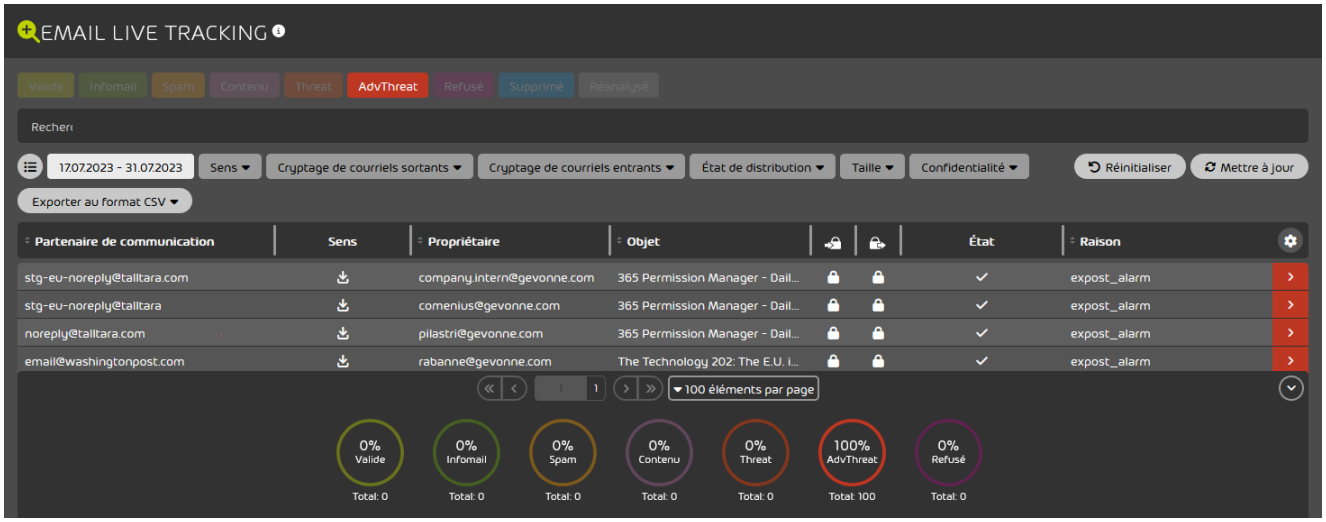


Illustration 260 : Catégorie AdvThreat

L'ATP avertit les délégués à la sécurité des entreprises des événements liés à la sécurité survenus à deux moments :

- Immédiatement après la réception des courriels déclencheurs avec des Real-Time Alert (voir Real-Time Alert à la page 364).
- Immédiatement après la détection de nouvelles menaces dans des courriels déjà envoyés, grâce à Ex Post Alert (voir Ex Post Alert à la page 365).

Le diagramme suivant montre le rôle de l'ATP dans le traitement des courriels par notre infrastructure.

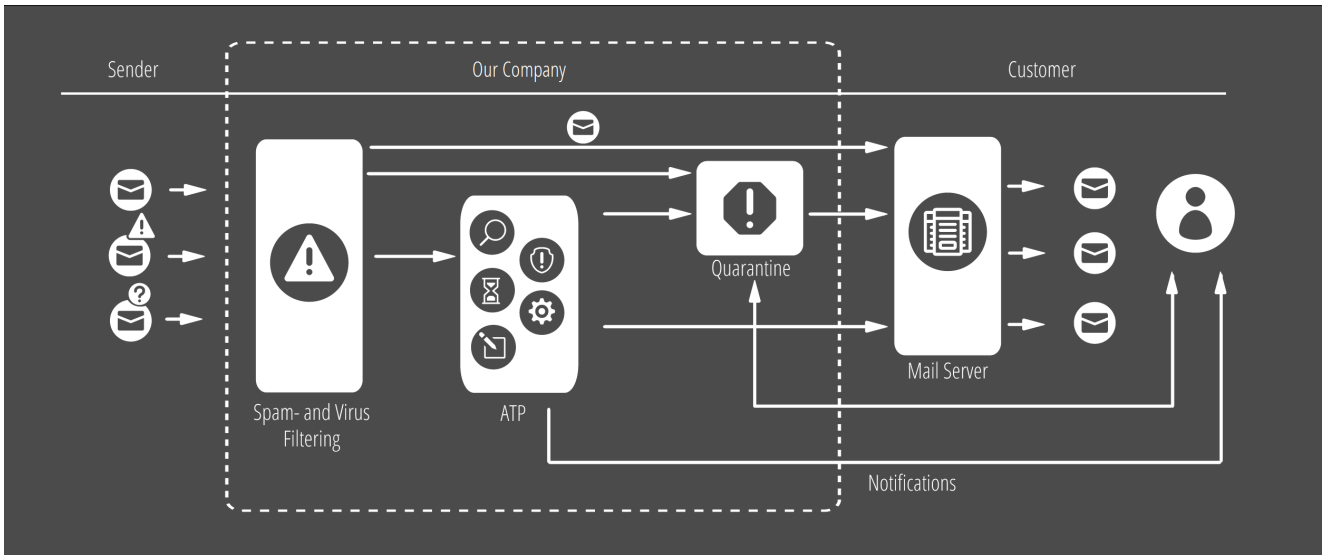


Illustration 261 : Fonctionnement de l’ ATP

Outre l'analyse automatique des courriels, tant à leur réception que dans le cadre de l'Ex Post Alert, l'ATP offre la possibilité d'effectuer des analyses manuelles des courriels contenant des fichiers exécutables. Grâce aux rapports ATP (voir Rapport ATP à la page 377), l'utilisateur reçoit, en plus d'une sécurité supplémentaire, des informations détaillées sur les courriels concernés sous la forme de rapports ATP (voir Rapport ATP à la page 77).

Pour qu'un client puisse utiliser Advanced Threat Protection, il faut qu'un administrateur active le service (voir Activer ATP à la page 365). Il est ensuite possible de gérer les destinataires des notifications de Real-Time Alert et d'Ex Post Alert (voir Saisir les destinataires des notifications à la page 367 et Supprimer des destinataires des notifications à la page 369). Les moteurs URL Rewriting et Targeted Fraud Forensics Filter doivent être activés séparément (voir Activer Secure Links à la page 371 et Activer le Targeted Fraud Forensics Filter à la page 373). En outre, les administrateurs peuvent déterminer les groupes d'utilisateurs auxquels le filtre Targeted Fraud Forensics doit être appliqué (voir Ajouter un groupe à la liste des groupes du TFFF à la page 375 et Supprimer un groupe de la liste des groupes du TFFF à la page 376).

Description des moteurs ATP

Advanced Threat Protection utilise un certain nombre de moteurs pour détecter et repousser les attaques.

Tableau 21 : Moteurs ATP

MOTEURS ATP	FONCTIONNEMENT ET AVANTAGES
Moteur Sandbox	Les pièces-jointes sont exécutées dans différents environnements système et leur comportement est analysé. S'il s'agit d'un maliciel, vous en serez notifié. Protège des ransomware et blended attacks.

MOTEURS ATP	FONCTIONNEMENT ET AVANTAGES
Secure Links	Secure Links empêche les utilisateurs d'être dirigés vers des pages Web malveillantes via des liens contenus dans des courriels. Si Secure Links est activé pour un client, les liens dans les courriels entrants des utilisateurs sont réécrits dès que les courriels parviennent à notre infrastructure. La réécriture permet une vérification ultérieure de la page Web par Secure Links. Dès qu'un utilisateur clique sur un lien réécrit dans un courriel, Secure Links vérifie la page Web à l'aide de nos bases de données Domain et URL Intelligence. Ces bases de données contiennent des milliards de jeux de données de phishing et de logiciels malveillants et sont continuellement élargies. Pendant les vérifications, des conseils de sécurité apparaissent dans le navigateur de l'utilisateur. Si la page Web passe la première vérification, Secure Links examine la page Web à la recherche d'autres indicateurs qui pourraient représenter un danger. Cela comprend notamment les liens intégrés vers des logiciels malveillants ou des formulaires de phishing. Ce n'est que si la page Web passe les deux vérifications que l'utilisateur sera redirigé vers la page Web. Dans le cas contraire, le navigateur web de l'utilisateur affiche une page avec l'un des messages suivants : • **Ce site web est bloqué** : En raison d'un comportement suspect, l'accès à la page Web demandée a été refusé. • **Avertissement** : Il se peut que la page Web demandé ne soit pas fiable, car une analyse complète de la page Web n'a pas été possible.

MOTEURS ATP	FONCTIONNEMENT ET AVANTAGES
URL Scanning	Les documents joints à un courriel (par ex. PDF, Microsoft) peuvent contenir des liens. Toutefois, les liens ne peuvent pas être remplacés, car cela violerait l'intégrité du document. L'URL Scanning Engine laisse le document dans sa forme originale et ne vérifie que la destination de ces liens.
QR Code Analyzer	Les images jointes à un courriel (par exemple PGN, JPEG, GIF et BMP) peuvent contenir des codes QR. Le QR Code Analyzer vérifie la destination du code QR et bloque le courriel si le code QR mène à une page web dangereuse.
Freezing	Les courriels ne pouvant être classés immédiatement mais suspects sont retenus par freezing sur une courte période de temps. Une vérification supplémentaire avec des signatures mises à jour est ensuite effectuée. Protège des ransomware, blended attacks et des attaques de phishing.

MOTEURS ATP	FONCTIONNEMENT ET AVANTAGES
Targeted Fraud Forensics Filter	Le Targeted Fraud Forensics Filter détecte les attaques personnalisées ciblées sans maliciels ni liens. Les mécanismes de reconnaissance suivants sont utilisés pour cela : • Intention Recognition System : Alerte pour les modèles de contenu qui suggèrent une intention malveillante. • Fraud Attempt Analysis : Vérifie l'authenticité et l'intégrité des métadonnées et du contenu des courriels. • Identity Spoofing Recognition : Détection et blocage de fausses identités d'expéditeurs. • Spy-Out Detection : Défense contre les attaques d'espionnage pour obtenir des informations sensibles. • Feign Facts Identification : Analyse du contenu des messages sur la base de faits simulés. • Targeted Attack Detection : Détection d'attaques ciblées sur des individus. Ce moteur doit être activé séparément (voir Activer le Targeted Fraud Forensics Filter à la page 373). Le Targeted Fraud Forensics Filter est appliqué aux groupes d'utilisateurs sélectionnés qui sont gérés dans une liste de groupes (voir Ajouter un groupe à la liste des groupes du TFFF à la page 375 et Supprimer un groupe de la liste des groupes du TFFF à la page 376).

Real-Time Alert

Real-Time Alert est une fonction de notification d'Advanced Threat Protection qui informe sur la raison de l'interception d'un courriel.

Dès qu'Advanced Threat Protection détecte une attaque, Real-Time Alert envoie immédiatement une notification à l'entreprise du client et l'informe d'une éventuelle menace. Le responsable reçoit alors des informations sur le type et la cible de l'attaque, l'expéditeur et la raison pour laquelle le courriel a été intercepté.

Des notifications sont envoyées dans les cas suivants :

- Le moteur Sandbox a trouvé un code malveillant (voir Moteur Sandbox).
- Secure Links a bloqué un site Web ou un téléchargement (voir Secure Links).
- URL Scanning a trouvé une URL corrompue (voir URL Scanning).
- Le Targeted Fraud Forensics Filter a filtré des courriels (voir Targeted Fraud Forensics Filter).

Sous **Paramètres de sécurité** > **Advanced Threat Protection**, des destinataires de notifications peuvent être ajoutés (voir Saisir les destinataires des notifications à la page 367) ou supprimés (voir Supprimer des destinataires des notifications à la page 369).

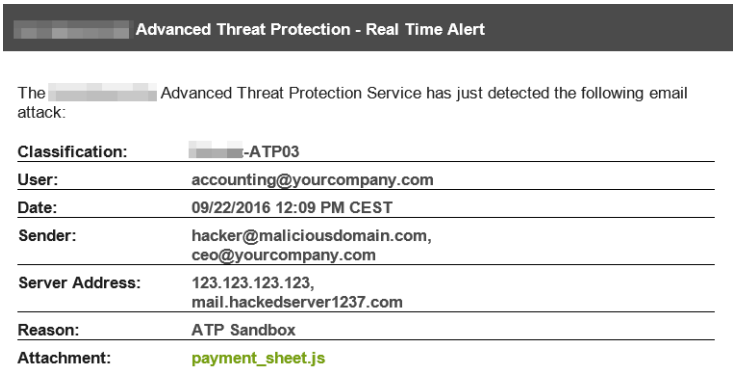


Illustration 262 : Notification en temps réel

Ex Post Alert

Grâce à Ex Post Alert, les équipes de sécurité informatiques des entreprises reçoivent une notification si un courriel déjà distribué a été classé comme malveillant.

Les destinataires d'Ex Post Alert reçoivent une évaluation détaillée de l'attaque afin de pouvoir immédiatement prendre des mesures telles que la vérification des systèmes ou la sensibilisation des employés.

Sous **Paramètres de sécurité** > **Advanced Threat Protection**, des destinataires de notifications peuvent être ajoutés (voir Saisir les destinataires des notifications à la page 367) ou supprimés (voir Supprimer des destinataires des notifications à la page 369).

REMARQUE :

Dès que l'Advanced Threat Protection est activée, Ex Post Alert est activée pour toutes les boîtes aux lettres des clients.

Configuration de base

Activer ATP

Vous avez activé la Spam and Malware Protection.

Vous pouvez activer Advanced Threat Protection pour protéger votre entreprise en temps réel contre les cyberattaques ciblées et individuelles.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer Advanced Threat Protection.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection**.

4. Actionnez le bouton **Activer Advanced Threat Protection**.

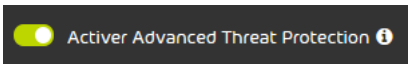


Illustration 263 : Activer Advanced Threat Protection

Une fenêtre de confirmation apparaît.

5. **ATTENTION :**

   Dès qu'Advanced Threat Protection est activé, une période d'essai gratuite de 30 jours démarre. Une fois la période d'essai terminée, le service devient payant.

   Cliquez sur **Confirmer**.

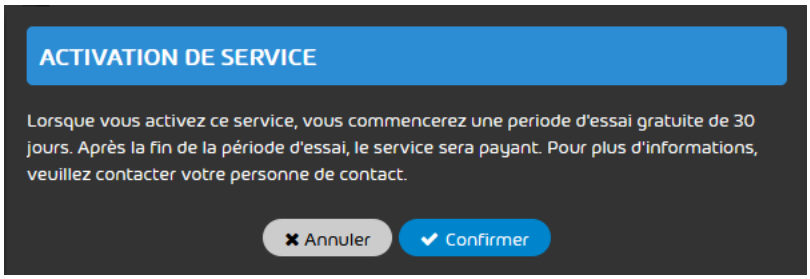


Illustration 264 : Confirmer

Advanced Threat Protection a été désactivée pour le domaine.

IMPORTANT :

L'activation activera tous les moteurs ATP (voir Description des moteurs ATP à la page 360), à l'exception de Secure Links et du Targeted Fraud Forensics Filter pour le domaine. Secure Links et le Targeted Fraud Forensics Filter doivent être activés séparément.

Vous pouvez ensuite gérer les destinataires des notifications d'Advanced Threat Protection (voir Saisir les destinataires des notifications à la page 367 et Supprimer des destinataires des notifications à la page 369). En outre, vous pouvez également activer que Engines Secure Links

et Targeted Fraud Forensics Filter (voir Activer Secure Links à la page 371 et Activer le Targeted Fraud Forensics Filter à la page 373).

Saisir les destinataires des notifications

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365).

Dans le module **Paramètres de sécurité** > **Advanced Threat Protection**, vous pouvez saisir les adresses courriel des utilisateurs qui doivent recevoir les notifications Real-Time Alert (voir Real-Time Alert à la page 364) et Ex Post Alert (voir Ex Post Alert à la page 365).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez ajouter le destinataire de notifications.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection**.
4. Cliquez sur **Ajouter destinataire**.

> **REMARQUE :**
>
> Il est particulièrement recommandé d'inscrire les délégués à la sécurité de votre entreprise comme destinataires.

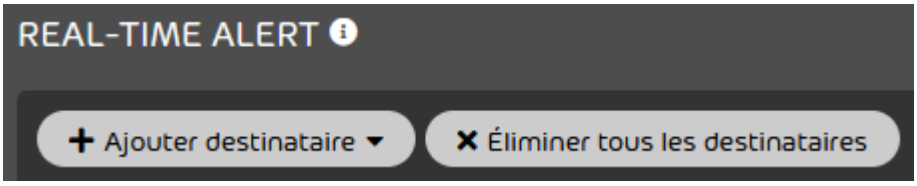


Illustration 265 : Ajouter des destinataires

Un affichage étendu s'ouvre.

5. Saisissez l'adresse courriel souhaitée dans le champ de saisie.

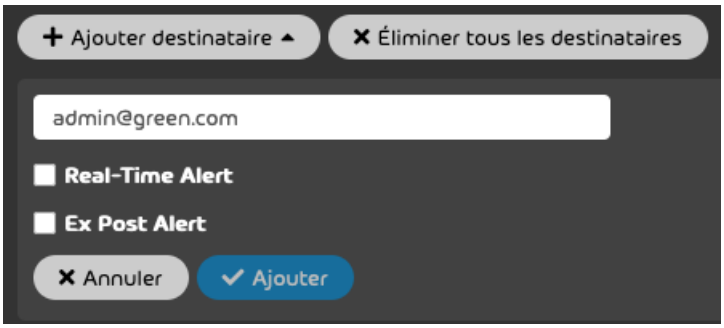


Illustration 266 : Saisir l' adresse courriel

6. Cochez les cases des types de notifications que le destinataire doit recevoir. Vous avez les options suivantes :

   - **Real-Time Alert** (voir Real-Time Alert à la page 364)
   - **Ex Post Alert** (voir Ex Post Alert à la page 365)

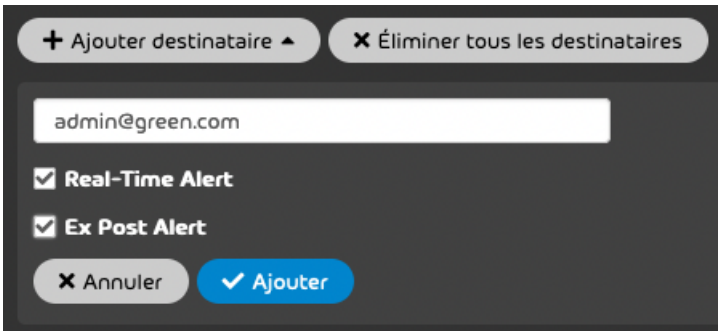


Illustration 267 : Sélectionner les types de notification

7. Cliquez sur **Ajouter**.

L'adresse courriel est ajoutée à la liste **Destinataires de notifications**. Les coches dans les colonnes **Ex Post Alert** et **Real-Time Alert** indiquent que le destinataire reçoit des notifications de ce type.

Illustration 268 : Destinataire ajouté

Une adresse courriel des utilisateurs qui doivent recevoir les notifications Real-Time Alert et/ou Ex Post Alert a été saisie.

Supprimer des destinataires des notifications

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365) et saisi des destinataires pour les notifications (voir Saisir les destinataires des notifications à la page 367).

Dans le module **Paramètres de sécurité** > **Advanced Threat Protection**, vous pouvez supprimer des adresses courriel dans la liste des destinataires des notifications d'Advanced Threat Protection (voir Structure et fonction d' ATP à la page 357). Vous pouvez supprimer soit des adresses courriel individuelles, soit toutes les adresses courriel en une seule fois.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer un destinataire des notifications d'Advanced Threat Protection.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection**.

4. Pour supprimer un seul destinataire, suivez les étapes suivantes :

   a) Dans la liste **Destinataires de notifications**, sélectionnez l'adresse courriel que vous souhaitez supprimer.

Illustration 269 : Sélectionner une adresse courriel

   b) Cliquez sur le symbole de croix dans la ligne de l'adresse courriel que vous souhaitez supprimer.

L'adresse courriel est supprimée de la liste.

5. Pour supprimer tous les destinataires en même temps, suivez les étapes suivantes :

   a) Cliquez sur **Éliminer tous les destinataires**.

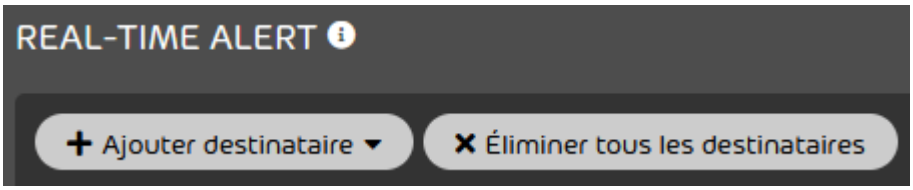


Illustration 270 : Supprimer tous les destinataires

- Une fenêtre de confirmation s'ouvre.

   b) Cliquez sur **Confirmer**.

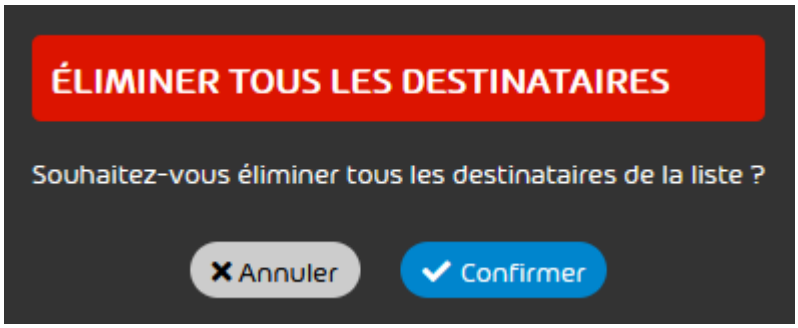


Illustration 271 : Confirmer

- Toutes les adresses courriel sont supprimées de la liste.

Des adresses courriel individuelles ou toutes les adresses courriel ont été supprimées de la liste des destinataires des notifications d'Advanced Threat Protection.

Activer Secure Links

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365).

Dans le module **Paramètres de sécurité** > **Advanced Threat Protection**, vous pouvez activer le moteur ATP Secure Links (voir Description des moteurs ATP à la page 360). Secure Links est activé par défaut pour tous les utilisateurs de votre domaine principal et vos domaines alias.

REMARQUE :

Si Secure Links ne doit pas être appliqué pour certains utilisateurs d'un domaine, ces exceptions doivent être communiquées au support technique.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer Secure Links.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection** dans le Control Panel.
4. Actionnez le bouton **Activer Secure Links** sous **SECURE LINKS**.

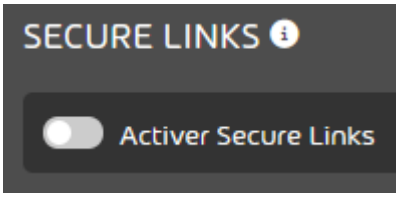


Illustration 272 : Activer Secure Links

Le bouton devient vert et une fenêtre de confirmation s'ouvre.

REMARQUE :

Secure Links est activé par défaut pour toutes les boîtes aux lettres de votre domaine principal et vos domaines alias. Si vous ne souhaitez pas activer Secure Links pour tous les domaines, veuillez contacter le support technique avant l'activation et leur indiquer quels domaines doivent être exclus de l'activation.

5. Cliquez sur **Confirmer**.

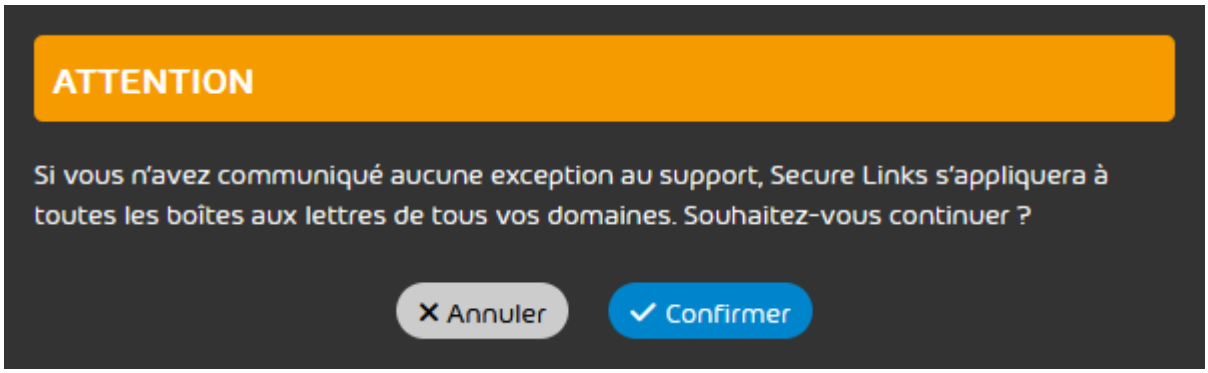


Illustration 273 : Confirmer

Secure Links a été activé pour toutes les boîtes aux lettres de votre domaine principal et de vos domaines alias qui n'ont pas été définis comme des exceptions.

Activer le Targeted Fraud Forensics Filter

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365) et créé des groupes d'utilisateurs (voir le chapitre « Groupes » dans le manuel du Control Panel). Vous avez activé la vérification SPF (voir le chapitre « Activer la vérification SPF » dans le manuel du Control Panel).

Dans le module **Paramètres de sécurité** > **Advanced Threat Protection**, vous pouvez activer le moteur ATP Targeted Fraud Forensics Filter (voir Description des moteurs ATP à la page 360) pour les groupes d'utilisateurs sélectionnés.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer le Targeted Fraud Forensics Filter.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection** dans le Control Panel.

4. Actionnez le bouton **Activer Targeted Fraud Forensics Filter** sous **TARGETED FRAUD FORENSICS FILTER**.

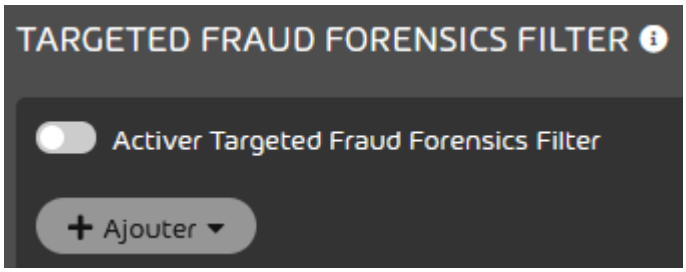


Illustration 274 : Activer le Targeted Fraud Forensics Filter

Le bouton devient vert. Le Targeted Fraud Forensics Filter est activé, mais il n'est pas encore appliqué aux groupes d'utilisateurs. Le bouton **Ajouter** est déverrouillé et un message apparaît.

5. Cliquez sur **Confirmer**.

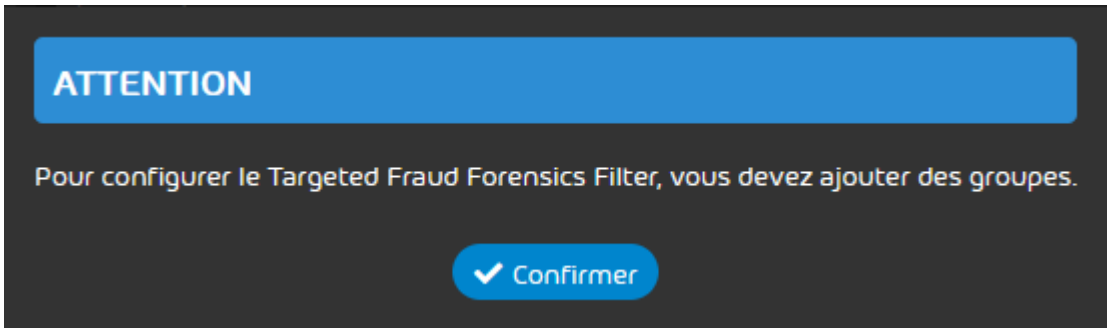


Illustration 275 : Confirmer

6. Ajoutez les groupes d'utilisateurs souhaités à la liste des groupes (voir Ajouter un groupe à la liste des groupes du TFFF à la page 375).

Le Targeted Fraud Forensics Filter est appliqué à tous les groupes d'utilisateurs ajoutés.

Le moteur ATP Targeted Fraud Forensics Filter a été activé.

Vous pouvez ensuite ajouter (voir Ajouter un groupe à la liste des groupes du TFFF à la page 375) ou supprimer des groupes (voir Supprimer un groupe de la liste des groupes du TFFF à la page 376) du Targeted Fraud Forensics Filter.

Ajouter un groupe à la liste des groupes du TFFF

Vous avez activé Targeted Fraud Forensics Filter (voir Activer le Targeted Fraud Forensics Filter à la page 373) et créé des groupes d'utilisateurs (voir le chapitre « Groupes » dans le manuel du Control Panel).

Le Targeted Fraud Forensics Filter n'est pas appliqué aux domaines mais aux groupes d'utilisateurs. Pour appliquer le Targeted Fraud Forensics Filter à un groupe, vous devez ajouter ce groupe à la liste des groupes du Targeted Fraud Forensics Filter.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez ajouter un groupe au Targeted Fraud Forensics Filter.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection** dans le Control Panel.
4. Dans la section **TARGETED FRAUD FORENSICS FILTER**, cliquez sur **Ajouter**.

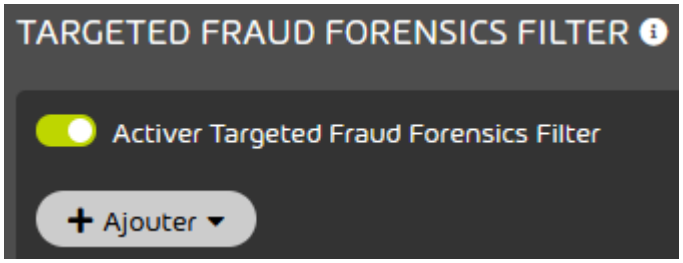


Illustration 276 : Ajouter un groupe

Un affichage étendu s'ouvre.

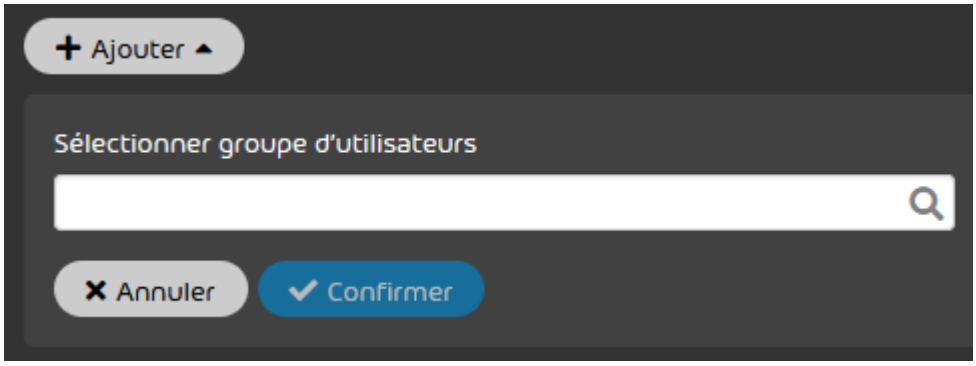


Illustration 277 : Vue élargie

5. Saisissez le nom du groupe souhaité dans le champ de recherche.

Un menu déroulant avec les résultats de la recherche s'ouvre.

6. Sélectionnez le groupe d'utilisateurs.
7. Cliquez sur **Confirmer**.

Illustration 278 : Confirmer

Le groupe est ajouté à la liste des groupes. Le Targeted Fraud Forensics Filter sera désormais appliqué à toutes les boîtes aux lettres de ce groupe.

Un groupe a été ajouté à la liste des groupes du Targeted Fraud Forensics Filter.

Vous pouvez ensuite supprimer le groupe de la liste des groupes du Targeted Fraud Forensics Filter (voir Supprimer un groupe de la liste des groupes du TFFF à la page 376).

Supprimer un groupe de la liste des groupes du TFFF

Vous avez activé le Targeted Fraud Forensics Filter (voir Activer ATP à la page 365) et ajouté des groupes d'utilisateurs à la liste des groupes (voir Ajouter un groupe à la liste des groupes du TFFF à la page 375).

Le Targeted Fraud Forensics Filter est appliqué aux groupes d'utilisateurs. Pour ne plus appliquer le Targeted Fraud Forensics Filter à un groupe, vous devez supprimer ce groupe de la liste des groupes du Targeted Fraud Forensics Filter.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer un groupe du Targeted Fraud Forensics Filter.
3. Naviguez vers **Paramètres de sécurité** > **Advanced Threat Protection**.
4. Dans la section **TARGETED FRAUD FORENSICS FILTER**, sélectionnez le groupe souhaité dans la liste des groupes.

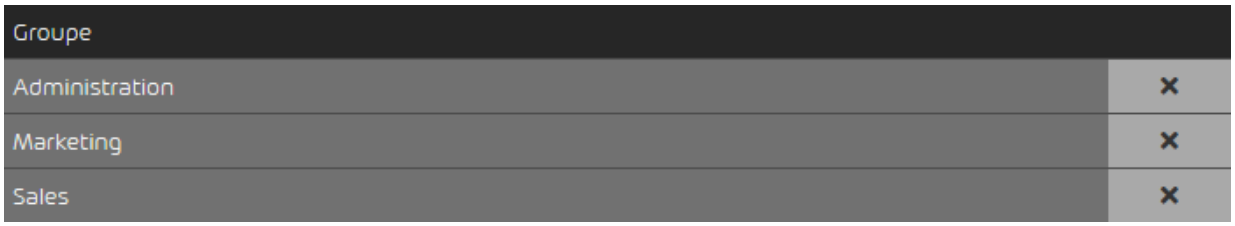


Illustration 279 : Sélectionner un groupe

5. Cliquez sur le symbole de croix à côté du groupe que vous souhaitez supprimer.

Le groupe est supprimé de la liste des groupes. Le Targeted Fraud Forensics Filter ne sera désormais plus appliqué aux boîtes aux lettres de ce groupe.

Un groupe de la liste des groupes du Targeted Fraud Forensics Filter a été supprimé.

Rapport ATP

Grâce au rapport ATP, les administrateurs peuvent vérifier les courriels. Le rapport ATP est déclenché manuellement (voir Démarrer le rapport ATP à la page 75) et vérifie les courriels avec des pièces jointes exécutables pour détecter les contenus malveillants. Le courriel sélectionné est analysé par le moteur Sandbox et un rapport détaillé est créé pour le courriel : le rapport ATP (voir Rapport ATP à la page 77).

Les clients qui n'ont pas souscrit à l'ATP peuvent également effectuer le rapport ATP. Pour ces clients, le nombre mensuel d'analyses est toutefois limité.

Comme les courriels des clients ATP sont déjà automatiquement analysés par le moteur Sandbox (voir Description des moteurs ATP à la page 360), le rapport ATP pour les clients ATP est principalement une mesure de sécurité supplémentaire (par exemple, avant la livraison manuelle de courriels classés **AdvThreat**). En outre, les clients ATP reçoivent des informations supplémentaires par le biais du rapport ATP.

Démarrer le rapport ATP

Vous avez activé Advanced Threat Protection (voir Activer ATP à la page 365).

Le rapport ATP (voir le chapitre « Rapport ATP » dans le manuel du Control Panel) vous permet d'analyser manuellement les courriels avec des pièces jointes exécutables dans le module **Email Live Tracking** (voir le chapitre « Email Live Tracking » dans le manuel du Control Panel) pour détecter les contenus malveillants.

REMARQUE :

Le rapport ATP n'est possible que pour les courriels comportant des pièces jointes exécutables (par exemple, des fichiers .exe).

ATTENTION :

Si vous n'avez pas souscrit à l'Advanced Threat Protection (voir le chapitre « Structure et fonction d'ATP » dans le manuel du Control Panel), vous pouvez bénéficier gratuitement de deux rapports ATP par mois. Vous ne pouvez effectuer d'autres rapports ATP que si vous avez souscrit à l'ATP payant.

1. Connectez-vous avec vos identifiants dans le Control Panel.
2. Si vous souhaitez accéder aux courriels d'un domaine au lieu de vos propres courriels, sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers le module **Email Live Tracking**.

4. Cliquez sur la flèche à droite du courriel souhaité.

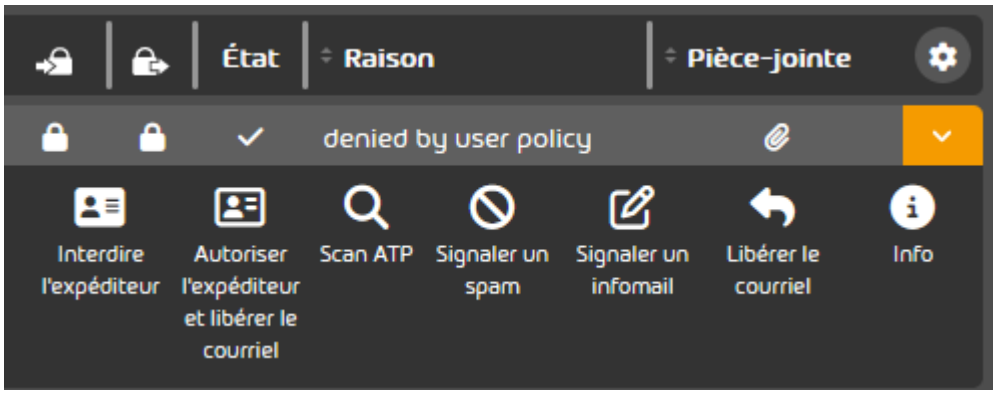


Illustration 280 : Rapport ATP dans Email Live Tracking

L'écran des fonctions étendues s'ouvre.

5. Cliquez sur **Scan ATP** pour lancer le rapport.

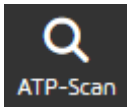


Illustration 281 : Démarrer le rapport ATP

Le rapport ATP a été lancé pour le courriel.

Une fois le rapport ATP terminé, vous pouvez consulter le rapport ATP dans la vue des fonctionnalités avancées du courriel sous la rubrique **Scan ATP** (voir Rapport ATP à la page 77).

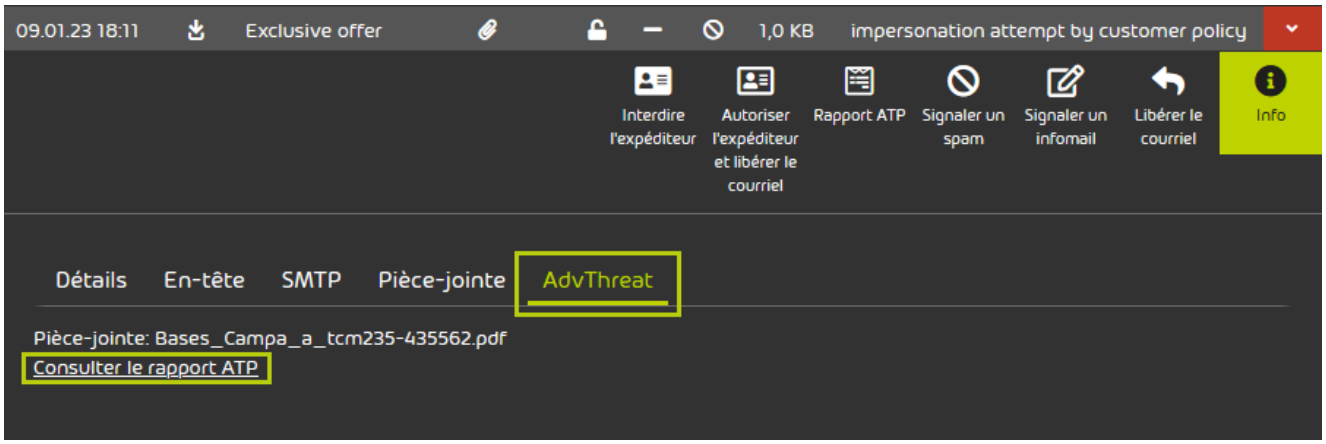


Illustration 282 : Ouvrir le rapport ATP

Rapport ATP

Le rapport ATP est un rapport détaillé qui est généré dès qu'un courriel a été vérifié avec le rapport ATP (voir le chapitre « Rapport ATP » dans le manuel du Control Panel et Démarrer le rapport ATP à la page 75). Le rapport ATP fournit des informations sur le courriel contrôlé. Les rapports ATP sont disponibles dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) pour les courriels vérifiés. Le rapport ATP d'un courriel peut être consulté dans le menu de courriel sous le point de menu **Rapport ATP** ou **Info** dans l'onglet **AdvThreat**.

Le rapport ATP est divisé en quatre fenêtres principales :

Summary

Vous trouverez ici un aperçu du fichier analysé. En outre, un **Score** de 0 à 10 est attribué au fichier. 0 signifie aucun danger et 10 est le niveau de danger le plus élevé.

Dans la section **Signatures**, le fichier est classé dans l'une des catégories suivantes en fonction de son comportement :

- information (vert)
- attention (jaune)
- avertissement (rouge)

Si vous cliquez sur une signature, les informations élargies au processus étendu s'affichent.

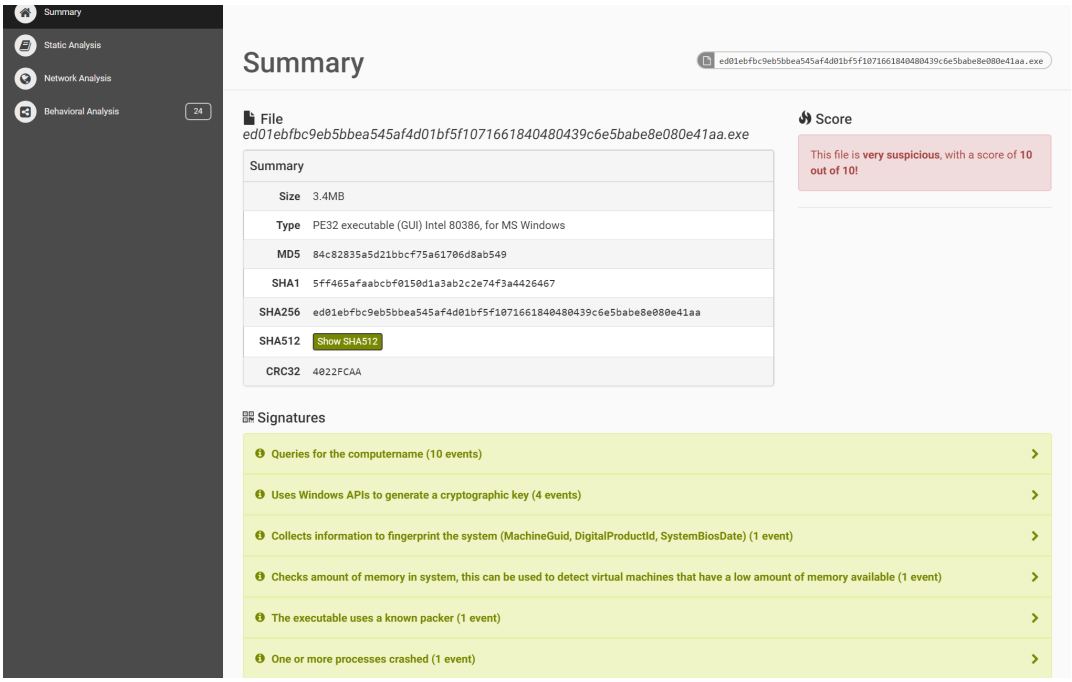


Illustration 283 : Aperçu rapport ATP

Static Analysis

L'analyse statique est à nouveau divisée en trois sous-catégories :

- Static Analysis – Analyse statique du fichier. Selon le format du fichier.
- Strings – Sortie des chaînes de caractères du fichier.
- Antivirus – Analyse du fichier par différents programmes antivirus.

Network Analysis

Dans l'analyse du réseau, l'ensemble du trafic réseau est analysé et répertorié selon les protocoles (par exemple HTTP, TCP, UDP).

Behavioral Analysis

L'analyse du comportement analyse le comportement du fichier au moment de l'exécution.

Tous les appels et processus de l'API système qui ont été enregistrés pendant l'analyse dynamique sandbox sont affichés.

Les résultats sont divisés en deux sections :

- Process Tree – Ici, les processus sont affichés dans l'ordre hiérarchique.
- Process Contents – Si vous sélectionnez un processus dans l'arborescence des processus, les requêtes API exécutées sont affichées ici par ordre chronologique.

Email Authentication

À propos de l'Email Authentication

L'Email Authentication offre aux administrateurs côté clients différentes possibilités pour authentifier les expéditeurs de courriels (voir Procédures d'authentification des expéditeurs à la page 384). Les procédures suivantes sont disponibles :

- Validation SPF (Sender Policy Framework) (voir Vérification SPF à la page 385)
- Validation DKIM et signature DKIM (DomainKeys Identified Mail) (voir Validation DKIM et signature DKIM à la page 397)
- Validation DMARC (Domain-based Message Authentication, Reporting and Conformance) (voir Validation DMARC à la page 402)

L'Email Authentication ne peut être utilisée que si la Spam and Malware Protection a été activée (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel). Avant d'activer la procédure, les administrateurs côté clients doivent vérifier les paramètres DNS de leurs propres domaines (voir Vérifier les paramètres DNS d'un domaine propre à la page 382).

Vérifier les paramètres DNS d'un domaine propre

Vous avez activé la Spam and Malware Protection (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

REMARQUE :

Vous pouvez vérifier les paramètres DNS uniquement pour les domaines pour lesquels la Spam and Malware Protection est activée.

Avant de paramétrer les procédures pour l'authentification des expéditeurs, vous devez vérifier si les paramètres DNS de vos domaines sont correctement configurés. Le statut des paramètres SPF, DKIM et DMARC de vos domaines est alors vérifié.

IMPORTANT :

Vous pouvez activer la vérification SPF (voir Vérification SPF à la page 385), la validation DKIM (voir Validation DKIM et signature DKIM à la page 397) et la validation DMARC (voir Validation DMARC à la page 402) uniquement pour vos domaines pour lesquels les paramètres DNS correspondants sont correctement configurés.

REMARQUE :

Pour savoir comment définir un enregistrement SPF, voir Définir un enregistrement SPF à la page 388.

Pour savoir comment définir un enregistrement CNAME, voir Définir un enregistrement CNAME à la page 397.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.

4. Cliquez sur **Mettre à jour les paramètres DNS** pour vérifier le statut des paramètres DNS de vos domaines.

Illustration 284 : Actualiser les paramètres DNS

Vous obtenez un aperçu sous forme de tableau du statut des paramètres DNS de vos domaines. Les trois résultats suivants sont possibles#:

✓	Les paramètres du domaine sont configurés correctement.
!	Aucun enregistrement n'est défini pour le domaine.
✗	Les paramètres du domaine ne sont pas configurés correctement.

Les paramètres DNS de vos domaines ont été vérifiés.

Vous pouvez ensuite activer des procédures d'authentification des expéditeurs (voir Procédures d'authentification des expéditeurs à la page 384).

Procédures d'authentification des expéditeurs

Les administrateurs côté client peuvent activer différentes procédures d'authentification d'expéditeurs de courriels pour leurs domaines. Les procédures suivantes sont disponibles :

- Vérification SPF à la page 385
- Validation DKIM et signature DKIM à la page 397
- Validation DMARC à la page 402

Ces procédures renforcent la protection de l'infrastructure des courriels des entreprises contre le spam et le phishing. Les administrateurs côté client peuvent utiliser les procédures séparément ou les combiner entre elles.

La combinaison de plusieurs procédures offre une protection supérieure. À titre d'exemple, sur les serveurs utilisant uniquement DKIM, le message indésirable peut être diffusé par un courriel avec une signature DKIM valide. Tant que ce courriel n'est pas modifié, il peut être expédié en masse à différentes personnes avec une signature DKIM valide. Pour éviter cela, il est possible d'utiliser également SPF. SPF vérifie l'origine du courriel. Ainsi, l'adresse IPv4 et le nom du domaine du serveur de messagerie sont vérifiés. SPF refuse les courriels des serveurs non autorisés. Il est alors impossible d'envoyer des messages indésirables par des courriels avec une signature DKIM valide.

En outre, les administrateurs côté client peuvent définir des exceptions aux procédures pour certains de leurs domaines (voir Ajouter des exceptions à la page 416).

Les courriels pour lesquels l'authentification de l'expéditeur a engendré une erreur sont rejetés ou marqués comme spam. Pour les courriels dont la vérification SPF, la validation DKIM ou la validation DMARC a échoué, certaines raisons de catégorisation sont indiquées dans le Control Panel (voir Raisons de catégorisation d' Email Authentication à la page 417).

Vérification SPF

SPF (Sender Policy Framework) est une procédure d'authentification des expéditeurs qui vérifie si l'adresse des expéditeurs d'un courriel est usurpée. Lors d'une vérification SPF, le serveur entrant vérifie si un courriel entrant provient d'un serveur autorisé. À cet effet, le serveur entrant vérifie si l'adresse IP du serveur sortant est saisie dans une entrée SPF dans la zone DNS du domaine de l'expéditeur. Dans une entrée SPF sont saisies les adresses IP du serveur qui sont autorisées pour l'envoi de courriels d'un domaine. Pour de plus amples informations sur la logique de la vérification SPF, voir Logique de la vérification SPF à la page 386.

Les administrateurs côté clients peuvent configurer la vérification SPF pour les courriels entrants de leurs domaines. Les administrateurs côté clients doivent définir à cet effet les enregistrements SPF, dans un premier temps, pour tous leurs domaines (voir Définir un enregistrement SPF à la page 388) pour lesquels ils veulent appliquer les vérifications SPF aux courriels entrants. Les administrateurs doivent ensuite activer la vérification SPF (voir Activer la vérification SPF à la page 389) et configurer les options avancées (voir Configurer les options étendues pour la vérification SPF à la page 392).

Le chapitre Élimination des erreurs à la page 395 explique comment les erreurs peuvent être corrigées lors des vérifications SPF.

Logique de la vérification SPF

La logique des vérifications SPF est décrite ci-après.

À la réception d'un courriel sur un serveur destinataire, l'adresse IP du serveur envoyé est synchronisée avec les enregistrements de l'enregistrement TXT du domaine de l'adresse courriel du serveur d'envoi. Si l'adresse IP du serveur d'envoi n'est pas incluse dans l'enregistrement TXT, une erreur est affichée. Lors de la vérification de l'enregistrement TXT, une distinction est faite entre les Hardfails et les Softfails, en fonction de leur gravité.

Les administrateurs côté clients peuvent décider des mesures à appliquer en fonction du type d'erreur (voir Activer la vérification SPF à la page 389). Si aucune erreur ne survient, le courriel est délivré de la manière habituelle.

REMARQUE :

Les exécutions suivantes reposent sur l'hypothèse selon laquelle les informations sur l'expéditeur de l'enveloppe (MAIL FROM) et les informations sur l'expéditeur de l'entête (From) doivent être vérifiées. Si une seule de ces informations doit être vérifiée, un seul contrôle a lieu, et le type d'échec de cette vérification est déterminant.

La logique suivante est prise en compte lors de l'analyse de l'enregistrement TXT :

1. La première étape consiste à vérifier simultanément les domaines indiqués dans l'enveloppe (MAIL FROM) et dans l'entête (From). Si l'une des vérifications contient une erreur, le type d'erreur est pris en compte lors de la prochaine étape. Si les deux vérifications contiennent des erreurs, le type d'erreur la plus grave est pris en compte pour l'étape suivante. Il existe trois possibilités.

   Tableau 22 : Possibilité 1 : les deux vérifications SPF entraînent des Softfails

   Si les vérifications SPF pour l'enveloppe et l'entête contiennent toutes deux des Softfails, un Softfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	~tous	Softfail
Entête (From)	~tous	Softfail

Tableau 23 : Possibilité 2 : les deux vérifications SPF entraînent des Hardfails

Si les vérifications SPF pour l'enveloppe et l'entête contiennent toutes deux des Hardfails, un Hardfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	-tous	Hardfail
Entête (From)	-tous	Hardfail

Tableau 24 : Possibilité 3 : les vérifications SPF entraînent différentes erreurs

Si les vérifications SPF pour l'enveloppe et l'en-tête contiennent différentes erreurs, un Hardfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	-tous	Hardfail
Entête (From)	~tous	Softfail

2. Lors de la deuxième étape, on vérifie les mesures que vous avez paramétrées pour un Hardfail ou un Softfail. Cette mesure est appliquée.

REMARQUE :

Dans des vérifications SPF, seuls les qualificatifs **-** et **~** sont pris en charge. Le qualificatif **-** représente le code de résultat Hardfail et le qualificatif **~** représente le code de résultat Softfail. Le qualificatif **?** n'est pas pris en charge.

Définir un enregistrement SPF

Vous pouvez définir un enregistrement SPF dans la zone DNS de votre domaine afin d'autoriser nos serveurs à envoyer des courriels au nom de votre domaine. Spam and Malware Protection (voir « Spam and Malware Protection » dans le manuel du Control Panel) peut, grâce à l'enregistrement SPF, reconnaître à temps les tentatives de tromperie, telles que le spoofing. Les destinataires extérieurs à votre organisation peuvent utiliser l'enregistrement SPF pour effectuer des contrôles SPF sur les courriels de votre domaine. En outre, vous avez besoin de l'enregistrement SPF afin que Email Authentication puisse effectuer des vérifications SPF (voir « Vérification SPF » dans le manuel du Control Panel) pour les courriels entrants.

IMPORTANT :

Enregistrez dans l'enregistrement SPF tous les serveurs qui peuvent envoyer des courriels depuis votre domaine.

REMARQUE :

Notre enregistrement SPF n'est pas nécessaire pour les clients qui ont configuré leur environnement principal avec l'option **IP/nom d'hôte**, mais qui n'ont enregistré aucune adresse de serveur de relais pour les courriels sortants. Pour obtenir de plus d'informations sur la configuration de l'environnement primaire, voir .

Vous devez définir vous-même l'enregistrement SPF dans la zone DNS de votre domaine. Pour obtenir de plus amples informations sur la façon dont vous pouvez définir correctement l'enregistrement SPF dans la zone DNS, veuillez contacter le support.

Activer la vérification SPF

Vous avez défini les enregistrements SPF valides dans la zone DNS de vos domaines (voir Définir un enregistrement SPF à la page 388). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

IMPORTANT :

Les vérifications SPF sont réalisées uniquement pour les domaines avec des enregistrements SPF valides.

IMPORTANT :

La vérification SPF ne peut être activée que si le client remplit l'une des conditions suivantes :

- Le client a configuré son environnement principal avec l'option **IP/nom d'hôte** et a enregistré des adresses de serveurs de relais pour les courriels sortants. Le client a également défini notre enregistrement SPF en plus de ses propres enregistrements SPF dans la zone DNS (voir Définir un enregistrement SPF à la page 388).
- Le client a configuré son environnement principal avec l'option **IP/nom d'hôte** mais n'a pas enregistré d'adresse de serveurs de relais pour les courriels sortants. Le client a défini ses propres enregistrements SPF dans la zone DNS.

Pour plus d'informations concernant la configuration de l'environnement principal, voir le chapitre « Procéder à la configuration de l'environnement principal » dans le manuel du Control Panel.

Vous pouvez activer la vérification SPF pour vérifier si l'adresse IP du serveur sortant d'un courriel entrant est saisie dans les enregistrements SPF du domaine de l'expéditeur et est autorisée à envoyer des courriels du domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.

3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Sous **Authentification d' expéditeur**, cochez la case **Activer la vérification SPF**.

Illustration 285 : Activer la vérification SPF

- Un message d'avertissement apparaît.

5. Cliquez sur **Confirmer**.

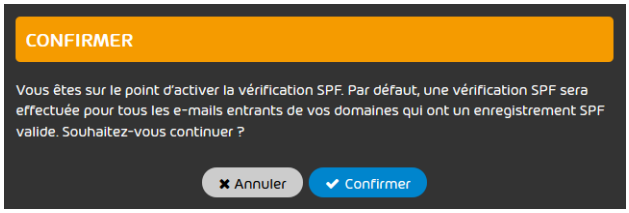


Illustration 286 : Confirmer

- La vérification SPF est activée pour tous les domaines qui se trouvent sous le domaine sélectionné et pour lesquels les enregistrements SPF corrects sont définis.

6. Sélectionnez dans quels cas une vérification SPF soit être réalisée.

   - Si tous les courriels entrants pour lesquels un enregistrement SPF est défini pour le domaine de l'expéditeur, sélectionnez **Pour tous les e-mails entrants**.

     REMARQUE :

     Cette variante est recommandée s'il y a, d'une manière générale, de nombreuses usurpations d'adresses provenant de différents domaines d'expéditeurs. L'utilisation de cette variante peut entraîner l'augmentation du nombre de faux positifs si des partenaires de communication n'ont pas défini correctement leurs enregistrements SPF.

   - Si seuls les courriels entrants envoyés par le domaine ou un domaine d'alias du destinataire doivent être vérifiés, sélectionnez **Uniquement pour les e-mails envoyés dans un de vos propres domaines**.

     REMARQUE :

     Seuls les courriels internes sont vérifiés. Cette variante est recommandée pour prévenir les attaques ciblées sous une adresse courriel usurpée de votre propre domaine.

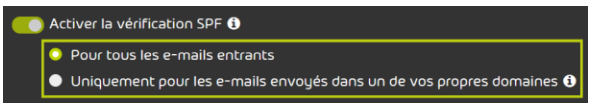


Illustration 287 : Sélectionner des courriels pour la vérification SPF

La vérification SPF est activée.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La vérification SPF a été activée.

Vous pouvez ensuite configurer les options étendues pour la vérification SPF (voir Configurer les options étendues pour la vérification SPF à la page 392).

Configurer les options étendues pour la vérification SPF

Vous avez activé la vérification SPF (voir Activer la vérification SPF à la page 389).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des vérifications SPF (voir Vérification SPF à la page 385).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

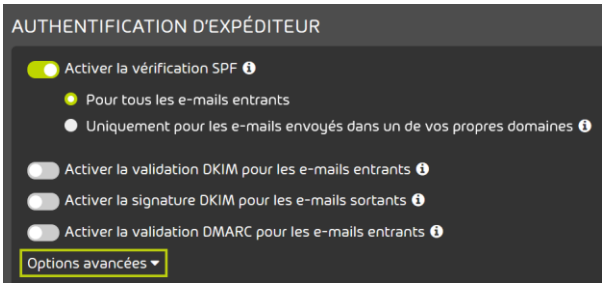


Illustration 288 : Ouvrir les options étendues

Un message d'avertissement apparaît.

5. **IMPORTANT :**

   Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

   Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 289 : Confirmer

6. Facultatif : Sous **Comportement après un échec sévère**, indiquez la conduite à tenir après un Hardfail SPF. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Ne prendre aucune mesure** : le Hardfail SPF ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

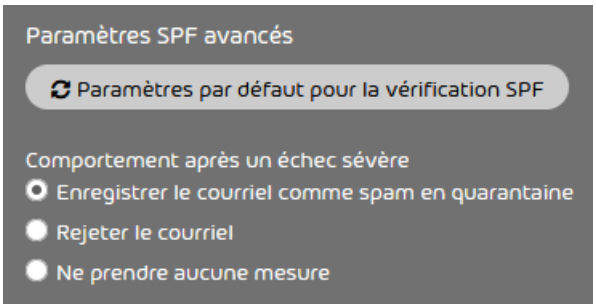


Illustration 290 : Sélectionner la procédure suite à un Hardfail SPF

7. Facultatif : Sous **Comportement après un échec partiel**, indiquez la conduite à tenir après un Softfail SPF. Vous avez trois options :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Ne prendre aucune mesure** : le Softfail SPF ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

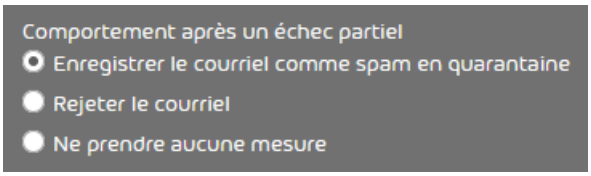


Illustration 291 : Sélectionner la procédure suite à un Softfail SPF

8. Facultatif : Sous **Analyse**, définissez les composants des courriels à analyser. Vous avez les options suivantes :

   - **Analyser uniquement 'envelope from'**
   - **Analyser uniquement 'header from'**
   - **Analyser 'envelope from' et 'header from'**

> **REMARQUE :**
>
> Si les deux indications sont vérifiées, la sécurité est améliorée, mais le nombre de faux positifs augmente également.

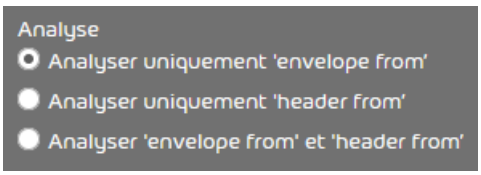


Illustration 292 : Configurer l' analyse

9. Facultatif : Pour réinitialiser les paramètres SPF aux réglages par défaut, cliquez sur **Paramètres par défaut pour la vérification SPF**.

> **REMARQUE :**
>
> Avec les réglages par défaut, après un Hardfail SPF et un Softfail SPF, les courriels sont mis en quarantaine et seul « Envelope-From » est analysé.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options avancées pour la vérification du SPF ont été configurées.

Élimination des erreurs

Les erreurs suivantes lors des vérifications SPF peuvent être corrigées :

- Erreur due aux vérifications SPF lors de l'envoi de courriels (voir Élimination des erreurs : Problèmes lors de l' envoi de courriels avec une entrée SPF configurée à la page 395)
- Erreur due aux vérifications SPF lors de la réception de courriels (voir Élimination des erreurs : Problèmes lors de la réception de courriels avec des vérifications SPF à la page 396)

Élimination des erreurs : Problèmes lors de l' envoi de courriels avec une entrée SPF configurée

Condition :

L'une des conditions suivantes est remplie :

- Les vérifications SPF sont exécutées chez vous, uniquement lorsque le domaine de l'expéditeur correspond au domaine du destinataire. Les courriels internes entrants sont identifiés comme non valides par erreur.

- Votre partenaire de communication vous indique que les courriels de votre domaine sont identifiés comme non valides lors des vérifications SPF.

Problème : Enregistrement TXT propre erroné

Les adresses IP saisies dans l'enregistrement TXT de votre serveur de messagerie ne sont pas correctes ou sont manquantes.

Résolution : Modifier l' enregistrement TXT

Insérez les adresses IPv4 de votre serveur de messagerie à l'enregistrement TXT ou corrigez les adresses IPv4 erronées.

Élimination des erreurs : Problèmes lors de la réception de courriels avec des vérifications SPF

Condition :

Les vérifications SPF sont exécutées pour tous les courriels entrants pour lesquels un enregistrement TXT est défini pour le domaine de l'expéditeur. Les courriels entrants de certains domaines sont identifiés comme non valides par erreur.

Problème : Enregistrement TXT erroné du partenaire de communication

Résolution : Informer le partenaire de communication

Informez le partenaire de communication d'une configuration SPF potentiellement erronée.

Résolution : Autoriser les adresses IP

1. Ouvrez le Control Panel.
2. Sélectionnez le domaine concerné dans la sélection de l'espace.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs autorisés**.
5. Dans le champ **Ajouter entrée**, saisissez l'adresse IPv4 du partenaire de communication.
6. Cliquez sur **Ajouter** pour confirmer votre saisie.

Validation DKIM et signature DKIM

DKIM (DomainKeys Identified Mail) est une procédure d'authentification de courriels vérifiant si les courriels ont été modifiés sur la voie de transfert. Avec une signature DKIM, une signature DKIM est ajoutée à l'en-tête d'un courriel sortant. Dès qu'un serveur reçoit un courriel avec une signature DKIM et qu'une validation DKIM est effectuée, le serveur destinataire interroge la clé publique saisie dans une entrée TXT dans la zone DNS du domaine de l'expéditeur. Cette clé permet de vérifier si la signature DKIM est correcte. La validation DKIM indique si un courriel a été modifié pendant la distribution.

Les expéditeurs des courriels entrants peuvent être authentifiés avec les validations DKIM. Pour cela, les administrateurs côté clients doivent activer d'abord la validation DKIM (voir Activer la validation DKIM à la page 398) et configurer ensuite les options étendues (voir Configurer les options étendues pour la validation DKIM à la page 399).

Les administrateurs côté client peuvent permettre aux destinataires des courriels sortants de leurs domaines d'effectuer des validations DKIM. Pour ce faire, les administrateurs doivent d'abord définir des enregistrements CNAME dans la zone DNS de leurs domaines, qui renvoient à nos enregistrements DKIM (voir Définir un enregistrement CNAME à la page 397). Les administrateurs doivent ensuite activer les signatures DKIM pour les courriels sortants de leurs domaines (voir Activer la signature DKIM à la page 401). Les courriels sortants qui sont acheminés par notre infrastructure sont alors signés par nos soins avec DKIM.

Définir un enregistrement CNAME

Si vous souhaitez utiliser DKIM (voir Validation DKIM et signature DKIM à la page 397), vous devez définir des enregistrements CNAME dans la zone DNS de votre domaine. Ces enregistrements renvoient à nos enregistrements DKIM. Les destinataires des courriels de votre domaine interrogent ces enregistrements afin d'obtenir la clé publique pour le décryptage de notre signature DKIM et d'autres informations nécessaires pour effectuer la validation DKIM.

1. Contactez le support technique pour obtenir les enregistrements CNAME.
2. Définissez les enregistrements CNAME dans la zone DNS de votre domaine.

Les enregistrements CNAME ont été définis dans la zone DNS de votre domaine.

Vous pouvez ensuite activer la validation DKIM (voir Activer la validation DKIM à la page 398).

Activer la validation DKIM

Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Vous pouvez activer la validation DKIM (voir Validation DKIM et signature DKIM à la page 397) pour vérifier les signatures DKIM des courriels entrants.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. **IMPORTANT :**

   La validation DKIM peut être activée uniquement pour vos domaines avec des paramètres DKIM valides.

   Cochez la case **Activer la validation DKIM pour les e-mails entrants** sous **Authentification d'expéditeur**.

Illustration 293 : Activer la validation DKIM

La validation DKIM est activée pour les courriels entrants.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La validation DKIM pour les courriels entrants a été activée pour votre domaine.

Vous pouvez ensuite configurer les options étendues pour la validation DKIM (voir Configurer les options étendues pour la validation DKIM à la page 399).

Configurer les options étendues pour la validation DKIM

Vous avez activé la validation DKIM (voir Activer la validation DKIM à la page 398).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des validations DKIM (voir Validation DKIM et signature DKIM à la page 397).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

Illustration 294 : Ouvrir les options étendues

Un message d'avertissement apparaît.

5. **IMPORTANT :**

   Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

   Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 295 : Confirmer

6. Facultatif : Sous **Paramètres DKIM avancés**, indiquez la conduite à tenir après un échec DKIM. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.

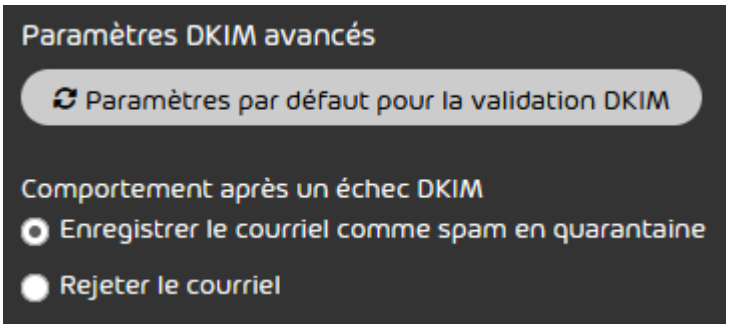


Illustration 296 : Sélectionner les options étendues

7. Facultatif : Pour réinitialiser les paramètres DKIM aux réglages par défaut, cliquez sur **Paramètres par défaut pour la validation DKIM**.

> **REMARQUE :**
>
> Avec les réglages par défaut, les courriels sont mis en quarantaines comme indésirables après un échec DKIM.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options étendues pour la validation DKIM ont été configurées.

Activer la signature DKIM

Vous avez défini les enregistrements CNAME valides dans la zone DNS de votre domaine (voir Définir un enregistrement CNAME à la page 397). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez activer la signature DKIM pour les courriels sortants de vos domaines afin que les destinataires des courriels puissent exécuter les validations DKIM.

1. Connectez-vous avec des identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. **IMPORTANT :**

   La validation DKIM peut être activée uniquement pour vos domaines avec des entrées DKIM valides.

   Cochez la case **Activer la signature DKIM pour les e-mails sortants** sous **Authentification d'expéditeur**.

Illustration 297 : Activer la signature DKIM

La signature DKIM a été activée pour les courriels sortants.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La signature DKIM a été activée pour les courriels sortants.

Validation DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) permet de définir le traitement d'un courriel entrant en fonction des résultats de la vérification SPF et de la validation DKIM ainsi que de l'alignement d'adresses et de domaines.

Une validation DMARC vérifie si un courriel entrant correspond à ce que sait le destinataire de l'expéditeur. Si un enregistrement DMARC a été défini dans la zone DNS du domaine de l'expéditeur, la validation DMARC suit la vérification SPF et la validation DKIM. La validation DMARC décide comment traiter le courriel en fonction des résultats de la vérification SPF et de la validation DKIM ainsi que de l'alignement d'adresses et de domaines dans l'Envelope-From et l'Header-From du courriel (alignement SPF) d'une part et des domaines dans l'Header-From et la signature DKIM (alignement DKIM) d'autre part. Pour de plus amples informations sur la matrice de décision DMARC, voir Matrice de décision DMARC à la page 406.

Les administrateurs côté clients peuvent configurer la validation DMARC pour les courriels entrants de leurs domaines. Pour cela, les administrateurs doivent d'abord définir un enregistrement DMARC dans la zone DNS de leurs domaines, (voir Définir un enregistrement DMARC à la page 402 et Balises dans les enregistrements DMARC à la page 403), activer la validation DMARC (voir Activer la validation DMARC à la page 411) et enfin configurer les options avancées (voir Configurer les options étendues pour la validation DMARC à la page 412).

Définir un enregistrement DMARC

Un enregistrement DMARC est la condition préalable pour que les validations DMARC (voir Validation DMARC à la page 402) puissent être réalisées pour les courriels d'un domaine. Vous pouvez définir un enregistrement DMARC pour votre domaine.

1. Dans la zone DNS de votre domaine, créez un enregistrement TXT avec le nom suivant. Remplacez **<domaine.tld>** par votre domaine.
   _dmarc.<domaine.tld>

2. Définissez dans l'enregistrement TXT la directive DMARC selon le schéma suivant à titre d'exemple. Remplacez **<utilisateur@domaine.tld>** par une adresse courriel.
v=DMARC1;p=quarantine;pct=100;rua=mailto:<utilisateur@domaine.tld>

> **IMPORTANT :**
>
> Le chapitre Balises dans les enregistrements DMARC à la page 403 contient une prévisualisation et des explications des balises qui peuvent être utilisées dans les enregistrements DMARC.

> **REMARQUE :**
>
> Les informations issues de l'enregistrement DMARC s'appliquent aux courriels expédiés aux destinataires en dehors du domaine. Les paramètres pour les courriels envoyés à des destinataires au sein du domaine peuvent être configurés dans le module **Email Authentication**.

Un enregistrement DMARC a été défini dans la zone DNS.

Balises dans les enregistrements DMARC

Les enregistrements DMARC se composent de balises. Les balises d'un enregistrement DMARC contiennent des exigences pour les validations DMARC de courriels expédiés par le domaine à un destinataire en dehors du domaine.

Le tableau suivant contient une prévisualisation et des explications des balises qui peuvent être utilisées dans les enregistrements DMARC. À l'exception de **v** et **p**, toutes les balises sont facultatives.

> **IMPORTANT :**
>
> Les balises **v** et **p** sont obligatoires.

BALISE	EXPLICATION	VALEURS POSSIBLES
v	Cette balise définit la version de protocole DMARC utilisée.	**v=DMARC1** **REMARQUE :** Pour cette balise, seul **v=DMARC1** est possible.
p	Cette balise définit de quelle manière comment traiter un courriel provenant du domaine si la validation DMARC échoue pour le courriel.	**p=quarantine** : le courriel est mis en quarantaine. **p=reject** : le courriel est refusé. **p=none** : aucune mesure n'est prise pour le courriel. **REMARQUE :** Nous recommandons **p=quarantine**.
pct	Cette balise définit le pourcentage des courriels soumis à des validations DMARC. Des chiffres compris entre 1 et 100 sont possibles pour cette balise.	**pct=100** **REMARQUE :** Nous recommandons **pct=100**, afin que les validations DMARC soient réalisées pour tous les courriels du domaine.

BALISE	EXPLICATION	VALEURS POSSIBLES
rua	Cette balise définit à quelle adresse courriel sont envoyés quotidiennement des rapports combinés sur les validations DMARC qui ont échoué.	**rua=mailto:<utilisateur@domaine.com>** Plutôt que **<utilisateur@domaine.com>**, l'adresse courriel à laquelle les rapports combinés doivent être envoyés est saisie.
ruf	Cette balise définit à quelle adresse courriel les rapports forensiques sont envoyés pour les courriels individuels pour lesquels la validation DMARC a échoué.	**ruf=mailto:<utilisateur@domaine.com>** Plutôt que **<utilisateur@domaine.com>**, l'adresse courriel à laquelle les rapports forensiques combinés doivent être envoyés est saisie.
sp	Cette balise définit comment traiter un courriel provenant d'un sous-domaine du domaine si la validation DMARC échoue pour le courriel.	**sp=quarantine** : le courriel est mis en quarantaine. **sp=reject** : le courriel est refusé. **sp=none** : aucune mesure n'est prise pour le courriel.
adkim	Cette balise définit le mode de calibrage pour les signatures DKIM (voir Validation DKIM et signature DKIM à la page 397). Le mode de calibrage détermine dans quelle mesure un courriel doit correspondre à la signature DKIM pour que le courriel soit accepté.	**adkim=r** : le mode de calibrage est souple. Une concordance partielle suffit. **adkim=s** : le mode de calibrage est strict. Une concordance complète est requise.

BALISE	EXPLICATION	VALEURS POSSIBLES
aspf	Cette balise définit le mode de calibrage pour les domaines de l'en-tête De et de l'envelope De d'un courriel (voir Vérification SPF à la page 385). Le mode de calibrage détermine avec quelle précision les deux domaines doivent correspondre pour que le courriel soit accepté.	**aspf=r** : le mode de calibrage est souple. Une concordance partielle suffit. **aspf=s** : le mode de calibrage est strict. Une concordance complète est requise.

Matrice de décision DMARC

La matrice de décision DMARC indique la conduite à tenir avec les courriels entrants après la réussite ou l'échec des vérifications SPF et des validations DKIM.

Tableau 25 : Matrice de décision DMARC

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Réussi	Réussi	Réussi	Réussi	Envoyer
Réussi	Réussi	Réussi	Échec	Réussi	Envoyer
Réussi	Réussi	Échec	Réussi	Réussi	Envoyer

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Réussi	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Réussi	Échec	Réussi	Réussi	Réussi	Envoyer
Réussi	Échec	Réussi	Échec	Réussi	Envoyer
Réussi	Échec	Échec	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Échec	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Échec	Réussi	Réussi	Réussi	Réussi	Envoyer
Échec	Réussi	Réussi	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Échec	Réussi	Échec	Réussi	Réussi	Envoyer

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Échec	Réussi	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Échec	Échec	Réussi	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Échec	Échec	Réussi	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Échec	Échec	Échec	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur
Échec	Échec	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l'expéditeur

Le résultat DMARC n'est positif que si la vérification SPF (voir Vérification SPF à la page 385) ou la validation DKIM (voir Validation DKIM et signature DKIM à la page 397) ainsi que l'alignement correspondant (SPF ou DKIM) ont réussi. Le courriel est transmis lorsque le résultat DMARC est positif. Autrement, en fonction des réglages dans le module **Email Authentication** (voir Configurer les options étendues pour la validation DMARC à la page 412) (le cas échéant), le courriel est mis en quarantaine comme spam, refusé, ou traité dans le Control Panel selon la directive DMARC du domaine de l'expéditeur.

Activer la validation DMARC

Vous avez défini des enregistrements SPF, DKIM et DMARC valides pour au moins l'un de vos domaines (voir Définir un enregistrement SPF à la page 388, Définir un enregistrement CNAME à la page 397 et Définir un enregistrement DMARC à la page 402). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Vous pouvez activer la validation DMARC pour définir le traitement des courriels entrants en fonction des résultats des vérifications SPF (voir Vérification SPF à la page 385) et des validations DKIM (voir Validation DKIM et signature DKIM à la page 397).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. **IMPORTANT :**

   La validation DMARC peut être activée uniquement pour vos domaines avec des enregistrements SPF, DKIM et DMARC valides.

   Cochez la case **Activer la validation DMARC pour les courriels entrants** sous **Authentification d'expéditeur**.

Illustration 298 : Activer la validation DMARC

La validation DMARC est activée pour les courriels entrants.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La validation DMARC a été activée pour les courriels entrants.

Vous pouvez ensuite configurer les options étendues en vue de la validation DMARC (voir Configurer les options étendues pour la validation DMARC à la page 412).

Configurer les options étendues pour la validation DMARC

Vous avez activé la validation DMARC (voir Activer la validation DMARC à la page 411).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des validations DMARC (voir Validation DMARC à la page 402).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

Illustration 299 : Ouvrir les options étendues

Un message d'avertissement apparaît.

5. **IMPORTANT :**

   Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

   Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 300 : Confirmer

6. Facultatif : Sous **Paramètres DMARC avancés**, indiquez le traitement à appliquer après un échec DMARC. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : Le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : Le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Appliquer la stratégie du domaine de l'expéditeur** : Après un échec DMARC, le comportement défini dans la directive DMARC du domaine expéditeur est appliqué. Il s'agit des paramètres par défaut.

   > **REMARQUE :**
   >
   > Si vous sélectionnez cette option, vous faites confiance aux politiques DMARC de tiers.

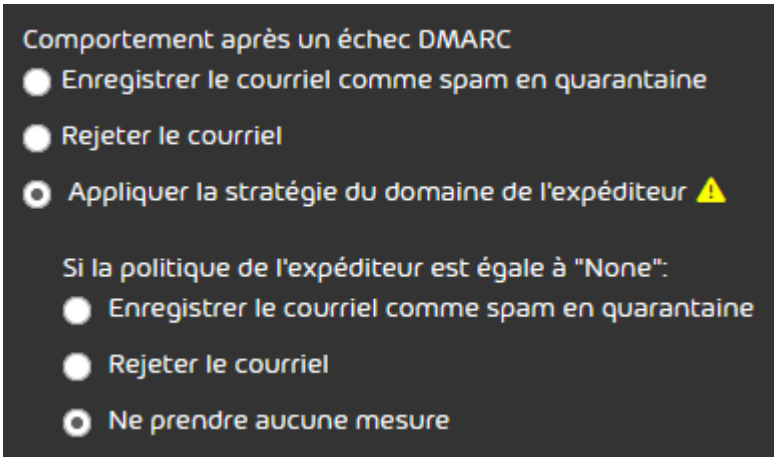


Illustration 301 : Choisir le comportement après un échec DMARC

Si l'option **Appliquer la stratégie du domaine de l'expéditeur** a été sélectionnée, d'autres paramètres s'affichent.

7. Si vous avez sélectionné l'option **Appliquer la stratégie du domaine de l'expéditeur**, passez à **Si la politique de l'expéditeur est égale à "None":** pour spécifier le comportement à

appliquer si la politique DMARC du domaine expéditeur est définie sur « None ». Vous avez les options suivantes :

- **Enregistrer le courriel comme spam en quarantaine** : Le courriel est classé comme courriel indésirable et mis en quarantaine.
- **Rejeter le courriel** : Le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
- **Ne prendre aucune mesure** : L'échec DMARC ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

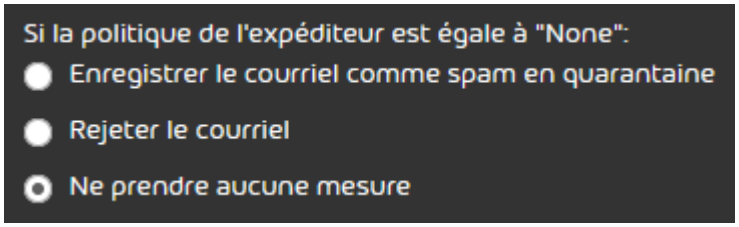


Illustration 302 : Comportement pour les directives d' expéditeur avec le paramètre « None »

8. Facultatif : Pour réinitialiser les paramètres DMARC aux réglages par défaut, cliquez sur **Paramètres par défaut pour la validation DMARC**.

> **REMARQUE :**
>
> Avec les paramètres par défaut, les courriels sont traités selon un DMARC-Fail conformément à la directive DMARC de l'expéditeur. Si la valeur **None** est entrée pour la directive DMARC de l'expéditeur (voir Définir un enregistrement DMARC à la page 402), aucune action ne sera effectuée par défaut.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options avancées pour la validation du DMARC ont été configurées.

Ajouter des exceptions

Vous avez activé des procédures d'authentification des expéditeurs dans le module **Email Authentication** (voir Procédures d' authentification des expéditeurs à la page 384).

Si vous avez activé la vérification SPF (voir Vérification SPF à la page 385), la validation DKIM (voir Validation DKIM et signature DKIM à la page 397) et/ou la validation DMARC (voir Validation DMARC à la page 402) et si vous souhaitez les désactiver pour l'un de vos domaines, ajoutez une exception.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Dans **Exceptions**, cliquez sur **Ajouter exception**.

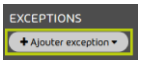


Illustration 303 : Ajouter une exception

Un affichage étendu s'ouvre.

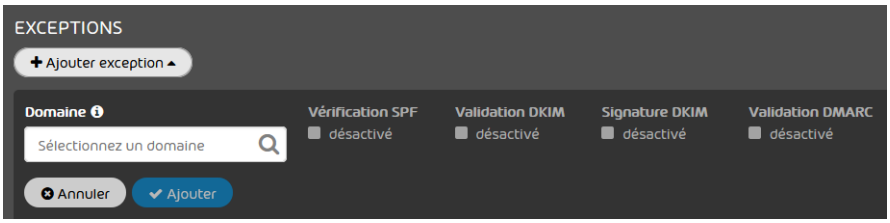


Illustration 304 : Vue élargie

5. Sous **Domaine**, sélectionnez un domaine pour lequel vous souhaitez activer l'exception.

> **REMARQUE :**
>
> Vous pouvez sélectionner uniquement les domaines pour lesquels la Spam and Malware Protection est activée.

6. Cochez la case sous la vérification que vous souhaitez désactiver pour le domaine.

> **REMARQUE :**
>
> Vous pouvez désactiver pour un domaine la vérification SPF, la validation DKIM ou la validation DMARC, uniquement si le domaine dispose des paramètres DNS valides correspondants. Les vérifications ne s'appliquent pas à tous les autres domaines.

7. Cliquez sur **Ajouter**.

L'exception est ajoutée et apparaît dans le tableau ci-dessous.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Une exception a été ajoutée à Email Authentication.

Raisons de catégorisation d' Email Authentication

Pour les courriels pour lesquels l'authentification de l'expéditeur avec Email Authentication a engendré une erreur, certaines raisons de catégorisation sont utilisées dans le Control Panel. Pour des informations sur d'autres raisons de catégorisation, voir le chapitre « Raisons de catégorisation » dans le mode d'emploi du Control Panel.

SPF

Les courriels pour lesquels une vérification SPF a montré qu'ils n'avaient pas été envoyés par un serveur enregistré dans le DNS sont mis en quarantaine comme indésirables, refusés ou distribués

en fonction de vos paramètres (voir Configurer les options étendues pour la vérification SPF à la page 392).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking**, quelle que soit la mesure exécutée, avec le motif **Envelope SPF Failure** et **Message Header SPF Failure**.

DKIM

Les courriels pour lesquels la validation DKIM a échoué sont mis en quarantaine comme indésirables ou refusés, en fonction de vos paramètres (voir Configurer les options étendues pour la validation DMARC à la page 412).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking** avec le motif **DKIM Failure**.

DMARC

Les courriels pour lesquels une validation DMARC a montré qu'ils ne correspondaient pas aux règles saisies pour SPF et/ou DKIM, sont mis en quarantaine comme indésirables ou refusés, en fonction de vos paramètres (voir Configurer les options étendues pour la validation DMARC à la page 412).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking** avec le motif **DMARC Failure**.

Quarantine Report

À propos du Quarantine Report

Le Quarantine Report est une fonction de Spam and Malware Protection (voir le chapitre « Spam and Malware Protection » dans le manuel du Control Panel), qui permet aux administrateurs côté clients de définir des rapports de quarantaine pour les utilisateurs de leurs domaines.

Le rapport de quarantaine est un rapport qui est soit créé individuellement pour un utilisateur, soit pour l'ensemble du domaine, et qui est distribué au destinataire par courriel. Les administrateurs

côté clients peuvent sélectionner une mise en page pour les rapports de quarantaine (voir Mises en page pour les rapports de quarantaine à la page 420). En fonction de la mise en page, différentes actions sur les courriels peuvent être effectuées dans les rapports de quarantaine (voir Actions sur les courriels dans les rapports de quarantaine à la page 425).

Le rapport de quarantaine répertorie tous les courriels catégorisés et courriels comme **Spam** et **Infomail** (voir le chapitre « Catégories de courriels » dans le manuel du Control Panel) qui n'ont pas été envoyés à l'utilisateur mais qui ont été mis en quarantaine. Si le destinataire du rapport de quarantaine dispose des droits nécessaires, il peut, s'il le souhaite, faire envoyer ces courriels ultérieurement (voir Actions sur les courriels dans les rapports de quarantaine à la page 425).

REMARQUE :

Dans le module **Spam and Malware Protection**, il est possible de paramétrer les courriels qui peuvent être envoyés aux utilisateurs (voir le chapitre « Autoriser ou interdire les actions d'utilisateur » dans le manuel du Control Panel).

REMARQUE :

Le nombre de courriels présentés est limité. Un rapport de quarantaine peut afficher maximum 1000 courriels.

Les rapports de quarantaine sont créés pour chacune des boîtes aux lettres principales. Si un utilisateur possède des boîtes aux lettres alias, il recevra un seul rapport de quarantaine répertoriant les courriels de la boîte aux lettres principale et des boîtes aux lettres alias. Dès qu'un utilisateur reçoit un courriel provenant d'un rapport de quarantaine (voir Envoyer un courriel depuis le rapport de quarantaine à la page 446), la boîte aux lettres à laquelle le courriel est adressé s'affiche. Les rapports de quarantaine sont également créés pour les boîtes aux lettres de renvoi (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel). Dans ce cas, chaque destinataire de renvoi reçoit une copie du rapport de quarantaine.

REMARQUE :

Pour les rapports de quarantaine qui ont été transmis des boîtes aux lettres de renvoi aux destinataires de renvoi, toutes les actions sur les courriels qui sont décrites dans le chapitre Actions sur les courriels dans les rapports de quarantaine à la page 425 ne sont pas possibles.

Les administrateurs côté clients peuvent activer le module **Quarantine Report** pour un domaine (voir Activer le Quarantine Report pour un domaine à la page 429) et le configurer (voir Configurer le Quarantine Report pour un domaine à la page 430). Les administrateurs peuvent également configurer le module **Quarantine Report** pour une seule boîte aux lettres séparément (voir Configurer le Quarantine Report pour une boîte aux lettres à la page 436). S'ils le souhaitent, les administrateurs peuvent également désactiver à nouveau le module **Quarantine Report** pour un domaine (voir Désactiver le Quarantine Report pour un domaine à la page 445).

Mises en page pour les rapports de quarantaine

Dans le module **Quarantine Report** (voir À propos du Quarantine Report à la page 418), les administrateurs côté clients peuvent sélectionner une mise en page pour les rapports de quarantaine de leurs domaines (voir Configurer le Quarantine Report pour un domaine à la page 430). La mise en page détermine les actions des courriels que les destinataires peuvent déclencher dans leurs rapports de quarantaine (voir Actions sur les courriels dans les rapports de quarantaine à la page 425).

REMARQUE :

Les informations du support du module **Personnalisation** s'affichent dans le pied de page des rapports de quarantaine (voir le chapitre « Enregistrer les informations du support dans le Control Panel » dans le manuel du Control Panel).

Les mises en page suivantes sont disponibles :

- **Mise en page standard** : cette mise en page est notre mise en page standard.

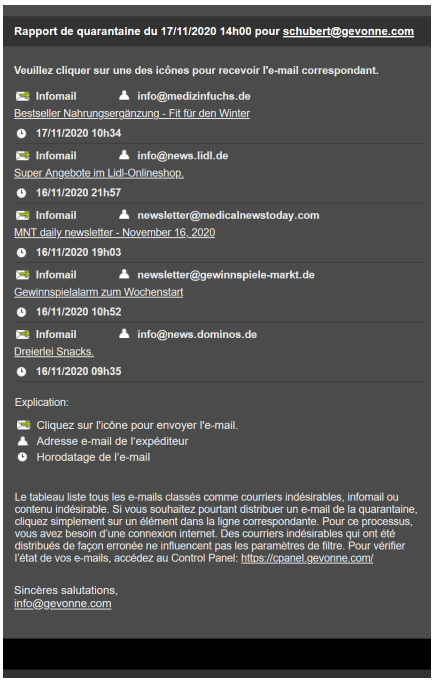


Illustration 305 : Mise en page standard

- **Mise en page standard avec l'aperçu du courriel** : cette mise en page est notre mise en page standard, avec des boutons supplémentaires pour la distribution et la prévisualisation des courriels (voir Prévisualisation de courriel à la page 93).

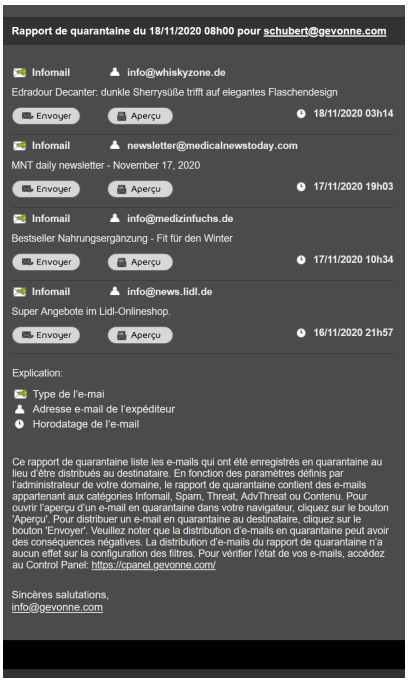


Illustration 306 : Mise en page standard avec l'aperçu du courriel

- **Inbox Manager avec l'aperçu du courriel et l'option d'exclusion** : cette mise en page est notre mise en page standard avec des boutons supplémentaires pour la distribution et la prévisualisation des courriels ainsi que pour l'exclusion des courriels d'un expéditeur des futurs rapports de quarantaine. Les rapports de quarantaine avec cette mise en page n'affichent pas les courriels des expéditeurs qui figurent sur le blacklist de l'utilisateur ou du domaine. Pour exclure les courriels d'un expéditeur des futurs rapports de quarantaine, le destinataire du rapport de quarantaine peut ajouter l'expéditeur d'un courriel mis en quarantaine à sa propre blacklist

en cliquant sur le bouton **Ne jamais afficher l'expéditeur** (voir le chapitre « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel).

IMPORTANT :

Cette mise en page ne s'affiche et ne peut être sélectionnée que si l'option **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine** a été activée dans les paramètres des rapports de quarantaine. Pour obtenir de plus amples informations sur la configuration des rapports de quarantaine, voir Configurer le Quarantine Report pour un domaine à la page 430.

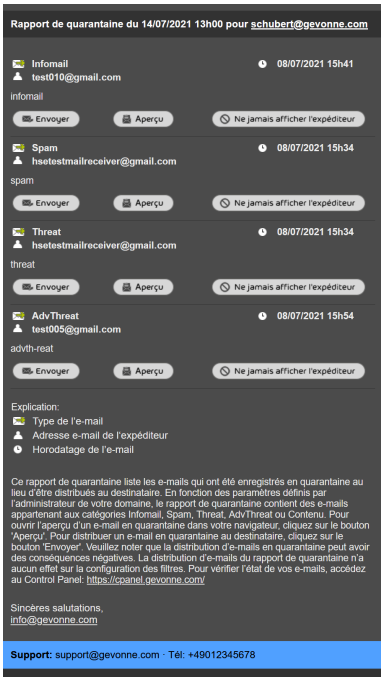


Illustration 307 : Inbox Manager avec l'aperçu du courriel et l'option d'exclusion

- **Mise en page pour bureau** : cette mise en page est optimale pour les PC de bureau car elle utilise la largeur de l'écran. Les rapports de quarantaine incluent des boutons pour la distribution des courriels et l'autorisation d'expéditeurs.

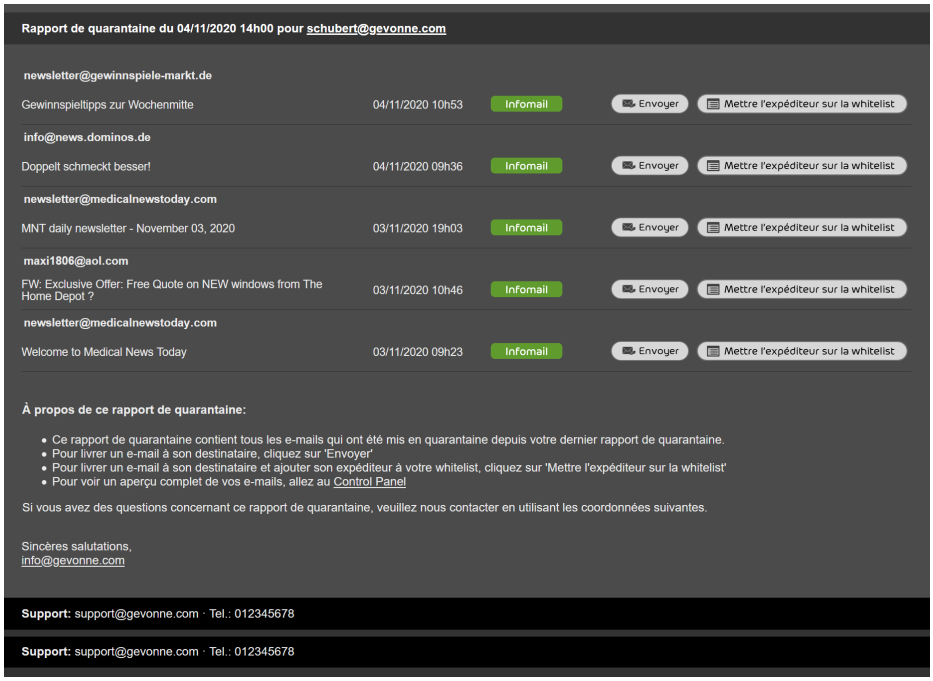


Illustration 308 : Mise en page pour bureau

- **Mise en page pour bureau avec l'aperçu du courriel** : cette mise en page est notre mise en page pour les bureaux, avec des boutons supplémentaires pour la prévisualisation des courriels (voir Prévisualisation de courriel à la page 93).

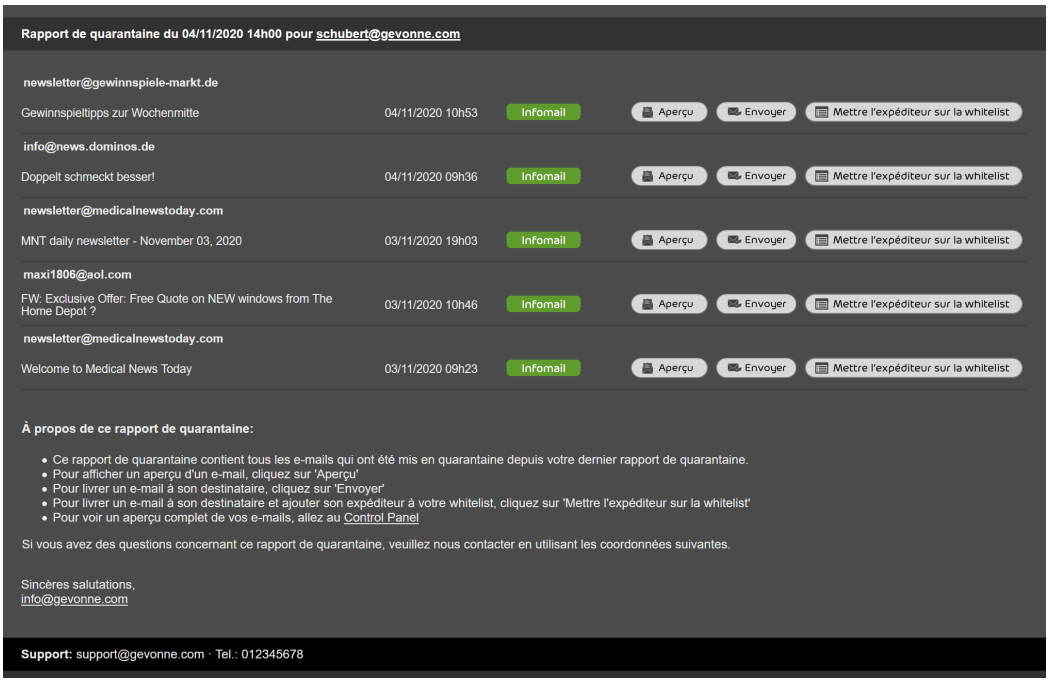


Illustration 309 : Mise en page pour bureau avec l'aperçu du courriel

Actions sur les courriels dans les rapports de quarantaine

Les rapports de quarantaine contiennent des boutons permettant d'exécuter certaines actions sur les courriels depuis le module **Email Live Tracking**. Les actions disponibles dépendent de la mise en page des rapports de quarantaine (voir Mises en page pour les rapports de quarantaine à la page 420). Les actions sont expliquées dans le tableau suivant et les mises en page dans lesquelles les actions sont disponibles sont détaillées.

Tableau 26 : Actions sur les courriels dans les rapports de quarantaine

ACTION	DISPOSITION	EXPLICATION
Envoyer	Mise en page standard Mise en page standard avec l'aperçu du courriel Inbox Manager avec l'aperçu du courriel et l'option d'exclusion Mise en page pour bureau Mise en page pour bureau avec l'aperçu du courriel	Les courriels sélectionnés sont envoyés au destinataire. **REMARQUE :** Dans le cas de rapports de quarantaine pour boîtes aux lettres de renvoi, les courriels sont envoyés à tous les destinataires de renvoi. Pour plus d'informations, voir le chapitre « Actions sur les courriels » dans le manuel du Control Panel.

ACTION	DISPOSITION	EXPLICATION
Mettre l'expéditeur sur la whitelist	**Mise en page pour bureau** **Mise en page pour bureau avec l'aperçu du courriel**	Les expéditeurs des courriels sélectionnés sont autorisés pour l'utilisateur et les courriels sont distribués. Tous les autres courriels des expéditeurs seront automatiquement distribués. **REMARQUE :** Cette action ne peut pas être effectuée dans les rapports de quarantaine pour les boîtes aux lettres de renvoi. Si un utilisateur essaie d'effectuer cette action, un message d'erreur apparaît.

ACTION	DISPOSITION	EXPLICATION
Aperçu	**Mise en page standard avec l'aperçu du courriel** **Inbox Manager avec l'aperçu du courriel et l'option d'exclusion** **Mise en page pour bureau avec l'aperçu du courriel**	Une nouvelle fenêtre propose un lien crypté permettant d'accéder à un service web où le contenu du courriel sélectionné s'affiche de manière sécurisée. Les images, liens et autres contenus actifs provenant du courriel sont désactivés ou remplacés par des caractères de remplacement sécurisés. Si nécessaire et dans la mesure du possible, la mise en page et le codage du courriel sont légèrement modifiés pour afficher le contenu du courriel. Pour plus d'informations, voir le chapitre « Prévisualisation de courriel » dans le manuel du Control Panel.

ACTION	DISPOSITION	EXPLICATION
Ne jamais afficher l'expéditeur	**Inbox Manager avec l'aperçu du courriel et l'option d'exclusion**	L'expéditeur du courriel sélectionné est interdit (voir le chapitre « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel) au niveau du destinataire (voir le chapitre « Actions sur les courriels » dans le manuel du Control Panel). À l'avenir, les courriels de l'expéditeur ne seront plus répertoriés dans les rapports de quarantaine de l'utilisateur.

REMARQUE :

Cette action ne peut pas être effectuée dans les rapports de quarantaine pour les boîtes aux lettres de renvoi. Si un utilisateur essaie d'effectuer cette action, un message d'erreur apparaît.

Activer le Quarantine Report pour un domaine

Vous avez activé la Spam and Malware Protection (voir le chapitre « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Vous pouvez activer le module **Quarantine Report** (voir À propos du Quarantine Report à la page 418) pour un domaine afin que les utilisateurs du domaine reçoivent les rapports de quarantaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer le module **Quarantine Report**.
3. Naviguez vers **Paramètres de sécurité** > **Quarantine Report**.
4. **IMPORTANT :**

   Si vous souhaitez apposer un label blanc (Whitelabeling) aux rapports de quarantaine, saisissez toutes les informations requises dans le module **Personnalisation** avant d'activer le module **Quarantine Report**. Le rapport de quarantaine est modifié automatiquement à l'aide des informations de ce module. Si vous n'avez entré aucune information dans le module, le rapport de quarantaine n'est pas modifié.

   Actionnez le bouton **Activer Quarantine Report**.

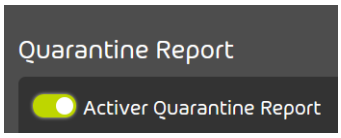


Illustration 310 : Activer le Quarantine Report

Le bouton devient vert.

Le module **Quarantine Report** a été activé pour un domaine.

Ensuite, vous pouvez configurer le module **Quarantine Report** pour le domaine (voir Configurer le Quarantine Report pour un domaine à la page 430).

Configurer le Quarantine Report pour un domaine

Vous avez activé le module **Quarantine Report** pour le domaine (voir Activer le Quarantine Report pour un domaine à la page 429).

Vous pouvez configurer les rapports de quarantaine pour un domaine dans le module **Quarantine Report** (voir À propos du Quarantine Report à la page 418).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Naviguez vers **Paramètres de sécurité** > **Quarantine Report**.
3. **IMPORTANT :**

   Par défaut, tous les utilisateurs du domaine reçoivent des rapports de quarantaine individuels à leurs propres adresses courriel. En alternative, vous pouvez également générer un rapport de quarantaine pour le domaine entier. Si un rapport de quarantaine pour le domaine entier est généré, les utilisateurs ne recevront aucun rapport de quarantaine.

   Facultatif : Pour générer un rapport de quarantaine pour l'ensemble du domaine, actionnez le bouton **Générer un rapport de quarantaine pour le domaine entier**.

Illustration 311 : Générer un rapport de quarantaine pour le domaine entier

Le champ **Adresse de destination pour le rapport de quarantaine** apparaît.

4. **IMPORTANT :**

   L'adresse courriel dans le champ **Adresse de destination pour le rapport de quarantaine** ne doit pas déjà être saisie comme destinataire du rapport de quarantaine d'un autre client.

   Facultatif : Dans le champ **Adresse de destination pour le rapport de quarantaine**, saisissez l'adresse courriel à laquelle le rapport de quarantaine sera envoyé.

5. Sélectionnez une mise en page sous **Options de mise en page pour les rapports de quarantaine** pour les rapports de quarantaine (voir Mises en page pour les rapports de quarantaine à la page 420).

   - **Mise en page standard**
   - **Mise en page standard avec l'aperçu du courriel**
   - **Inbox Manager avec l'aperçu du courriel et l'option d'exclusion**

     IMPORTANT :

     Cette mise en page ne s'affiche et ne peut être sélectionnée que si l'option **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine** a été activée dans les paramètres des rapports de quarantaine.

   - **Mise en page pour bureau**
   - **Mise en page pour bureau avec l'aperçu du courriel**

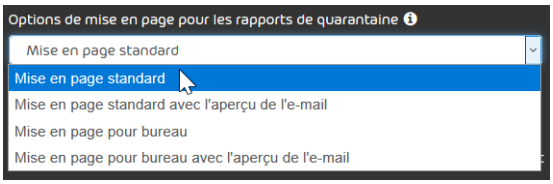


Illustration 312 : Sélectionner la mise en page

REMARQUE :

Les mises en page avec prévisualisation de courriel ne sont pas disponibles pour les rapports de quarantaine générés pour l'ensemble du domaine.

REMARQUE :

Pour plus d'informations concernant la prévisualisation du courriel, voir le chapitre « Prévisualisation de courriel » dans le manuel du Control Panel.

6. Facultatif : Si vous souhaitez supprimer des références au Control Panel depuis les rapports de quarantaine, actionnez le bouton **Afficher un lien vers le Control Panel dans les rapports de quarantaine**.

> **REMARQUE :**
>
> Par défaut, les rapports de quarantaine se réfèrent au Control Panel.

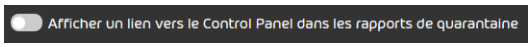


Illustration 313 : Supprimer le lien vers le Control Panel

Le bouton devient gris.

7. Cochez les cases des types de courriel qui doivent être décrits dans les rapports de quarantaine. Vous pouvez choisir parmi les types de courriel suivants.

- **Infomail**
- **Spam**
- **Threat et AdvThreat**
- **Contenu**

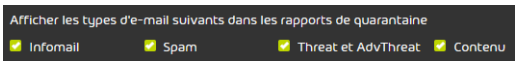
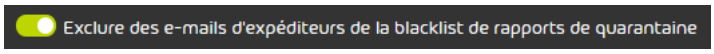


Illustration 314 : Sélectionner les types de courriel

8. Si vous souhaitez exclure des rapports de quarantaine les courriels provenant d'expéditeurs qui sont interdits pour le destinataire ou pour le domaine, actionnez le bouton **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine**.



IMPORTANT :

Si un rapport de quarantaine est généré pour l'ensemble du domaine (voir ci-dessus), seuls les courriels provenant d'expéditeurs qui sont interdits pour le domaine seront exclus. Les expéditeurs interdits des destinataires ne sont pas pris en compte.

Illustration 315 : Exclure des courriels d'expéditeurs interdits de rapports de quarantaine.

Le bouton est activé. La mise en page **Inbox Manager avec l'aperçu du courriel et l'option d'exclusion** est activée dans le menu déroulant **Options de mise en page pour les rapports de quarantaine**.

9. Sous **Moments de distribution**, sélectionnez les moments auxquels les rapports de quarantaine doivent être distribués. Vous pouvez cocher les cases des jours et heures souhaités ou cliquer sur les boutons suivants :

   - **Chaque heure** : toutes les heures sont sélectionnées.
   - **Chaque jour** : tous les jours sont sélectionnés.
   - **Les jours de la semaine** : tous les jours de lundi à vendredi sont sélectionnés.
   - **Désactiver** : aucun jour ou heure n'est sélectionné. Les rapports de quarantaine sont désactivés par défaut pour tous les utilisateurs du domaine.

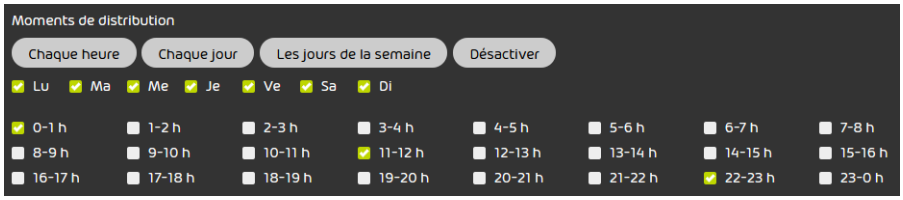


Illustration 316 : Sélectionner les heures

REMARQUE :

Aux moments de distribution sélectionnés, un rapport de quarantaine n'est envoyé que si de nouveaux courriels ont été mis en quarantaine depuis le dernier rapport de quarantaine.

10. **IMPORTANT :**

    Par défaut, les utilisateurs du domaine reçoivent les rapports de quarantaine aux moments de distribution qui ont été fixés pour le domaine. Si des moments de distribution ont été sélectionnés pour le domaine, par défaut, les utilisateurs ne peuvent pas modifier les moments de distribution pour leurs propres rapports de quarantaine.

    Si aucun moment de distribution n'a été sélectionné pour le domaine, les utilisateurs peuvent modifier les moments de distribution pour leurs propres rapports de quarantaine. Cette autorisation ne peut pas être désactivée.

    Facultatif : Pour permettre aux utilisateurs du domaine de modifier les moments de distribution de leurs rapports de quarantaine, actionnez le bouton **Autoriser les utilisateurs à modifier les moments de distribution de leurs propres rapports de quarantaine**.

Illustration 317 : Permettre aux utilisateurs d' adapter les moments de distribution

Le bouton devient vert.

11. Créez un texte personnalisé dans chaque langue dans laquelle les rapports de quarantaine doivent être remis (voir ICréer un texte personnalisé pour les rapports de quarantaine à la page 440).
12. Pour appliquer les modifications, cliquez sur **Enregistrer**.

Le module **Quarantine Report** a été configuré pour un domaine.

Vous pouvez ensuite configurer les rapports de quarantaine différemment pour une boîte aux lettres du domaine (voir Configurer le Quarantine Report pour une boîte aux lettres à la page 436).

Configurer le Quarantine Report pour une boîte aux lettres

Vous avez activé le module **Quarantine Report** pour le domaine (voir Activer le Quarantine Report pour un domaine à la page 429). Vous avez configuré le module **Quarantine Report** pour le domaine (voir Configurer le Quarantine Report pour un domaine à la page 430).

Dans le module **Paramètres client** > **Boîtes aux lettres**, vous pouvez configurer les rapports de quarantaine pour une boîte aux lettres différemment des autres boîtes aux lettres du domaine (voir Configurer le Quarantine Report pour un domaine à la page 430).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la zone de sélection, sélectionnez le domaine de la boîte aux lettres pour laquelle vous souhaitez configurer le module **Quarantine Report**.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.
4. Sélectionnez la boîte aux lettres dans la liste et cliquez sur la flèche à côté de la boîte aux lettres.

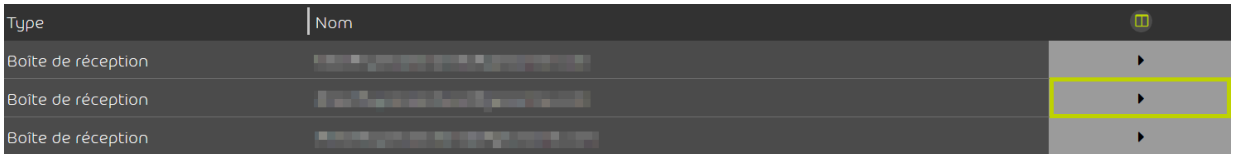


Illustration 318 : Afficher les paramètres avancés

Un menu s'ouvre.

5. Dans le menu, cliquez sur **Quarantine Report**.

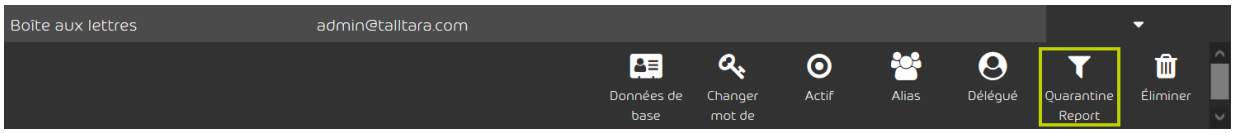


Illustration 319 : Menu

Les paramètres du module **Quarantine Report** pour la boîte aux lettres sont affichés. Si vous n'avez pas encore défini les paramètres du module **Quarantine Report** pour la boîte aux lettres, les paramètres du domaine sont prédéfinis ici.

6. Pour configurer le module **Quarantine Report** pour la boîte aux lettres, actionnez le bouton **Définir vos propres moments de distribution**.

Illustration 320 : Définir vos propres moments de distribution

- Le bouton devient vert. Vous pouvez désactiver le module **Quarantine Report** pour la boîte aux lettres ou modifier les moments de distribution des rapports de quarantaine.

7. Si vous souhaitez exclure des rapports de quarantaine les courriels provenant d'expéditeurs qui sont interdits pour le destinataire ou pour le domaine, actionnez le bouton **Exclure des courriels d'expéditeurs interdits de rapports de quarantaine**.

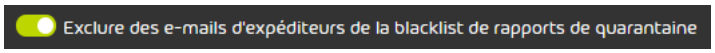


Illustration 321 : Exclure des courriels d'expéditeurs interdits de rapports de quarantaine

- Le bouton devient vert.

8. Si vous souhaitez désactiver le module **Quarantine Report** pour la boîte aux lettres, activez le bouton **Désactiver**.

Illustration 322 : Désactiver le Quarantine Report

- Tous les jours et moments de distribution sont désactivés pour la boîte aux lettres. Aucun rapport de quarantaine n'est distribué à la boîte aux lettres. Aucun autre paramètre n'est nécessaire.

9. Si le module **Quarantine Report** pour la boîte aux lettres reste activé, sélectionnez les jours où les rapports de quarantaine doivent être distribués. Sélectionnez au moins un jour.

   - Pour diffuser les rapports de quarantaine tous les jours, activez le bouton **Chaque jour**.
   - Pour recevoir les rapports de quarantaine quotidiennement du lundi au vendredi, activez le bouton **Les jours de la semaine**.
   - Cochez les cases des jours souhaités.

Illustration 323 : Sélectionner les jours

10. Sélectionnez les heures auxquelles les rapports de quarantaine doivent être distribués. Sélectionnez au moins une heure.

    - Pour diffuser les rapports de quarantaine toutes les heures, activez le bouton **Chaque heure**.
    - Cochez les cases des heures souhaitées.

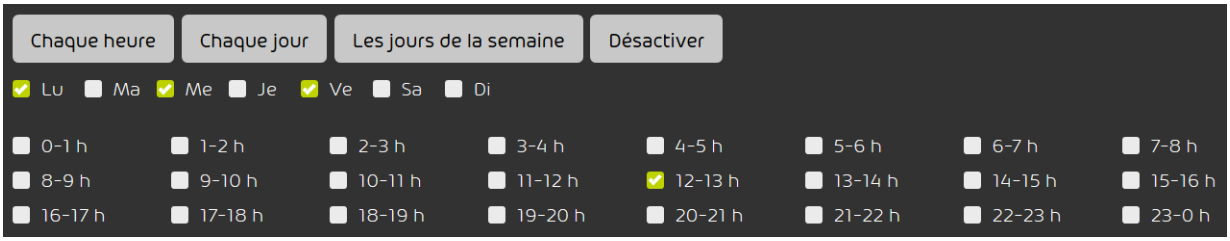


Illustration 324 : Sélectionner les heures

> **REMARQUE :**
>
> Aux moments de distribution sélectionnés, un rapport de quarantaine n'est envoyé que si de nouveaux courriels ont été mis en quarantaine depuis le dernier rapport de quarantaine.

Le module **Quarantine Report** a été configuré pour une boîte aux lettres.

ICréer un texte personnalisé pour les rapports de quarantaine

Vous avez activé le module **Quarantine Report** (voir Activer le Quarantine Report pour un domaine à la page 429).

Dans le module **Quarantine Report** (voir À propos du Quarantine Report à la page 418), vous pouvez adapter les rapports de quarantaine de votre domaine avec un texte personnalisé dans chaque langue prise en charge par le Control Panel. Le texte s'affiche dans le rapport de quarantaine sous la liste des courriels.

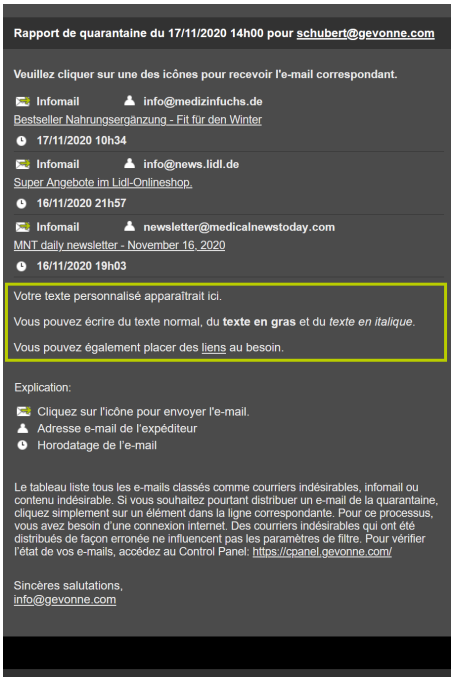


Illustration 325 : Exemple de texte personnalisé

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Naviguez vers **Paramètres de sécurité** > **Quarantine Report**.

3. Actionnez le bouton **Utiliser un texte personnalisé dans les rapports de quarantaine**.

Illustration 326 : Utiliser un texte personnalisé

Le bouton devient vert. La zone pour la création de textes personnalisés s'active.

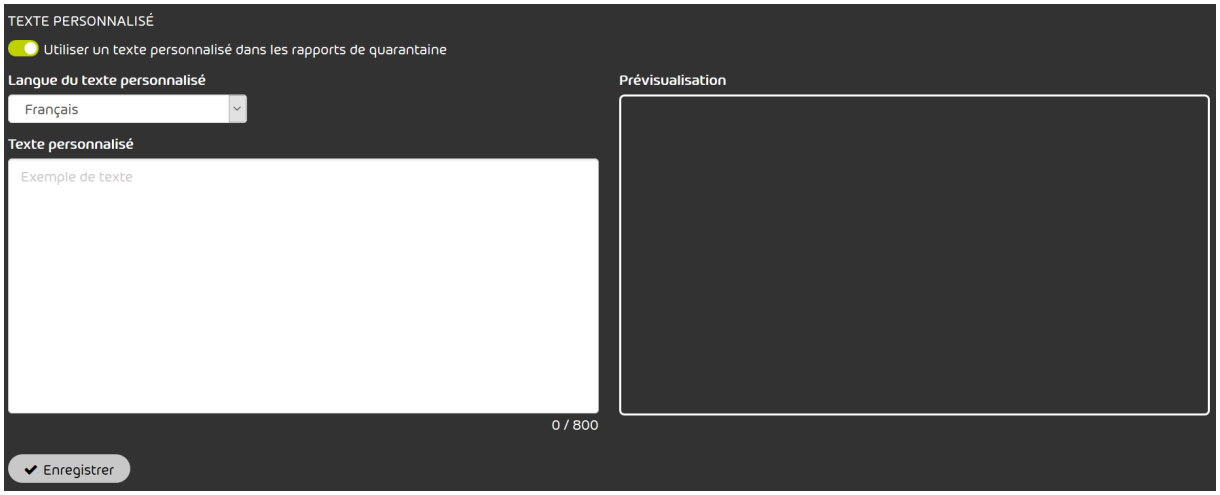


Illustration 327 : Éditeur de texte

4.

IMPORTANT :

Chaque utilisateur reçoit ses rapports de quarantaine dans la langue définie pour lui dans le Control Panel sous **Paramètres utilisateur** (voir Modifier le fuseau horaire et la langue à la page 34). Cette langue peut être différente de la langue par défaut du domaine dans le module **Tableau de bord des services** (voir Régler les valeurs par défaut pour le fuseau horaire et la langue à la page 145).

Pour chaque langue disponible, un texte personnalisé peut être créé. Les textes personnalisés sont ajoutés aux rapports de quarantaine dans la même langue. Si aucun texte personnalisé n'est enregistré pour une langue, les rapports de quarantaine sont envoyés dans cette langue sans texte personnalisé.

Sélectionnez la langue du texte personnalisé sous **Langue du texte personnalisé**.

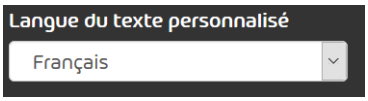


Illustration 328 : Langue du texte personnalisé

REMARQUE :

Si vous sélectionnez une autre langue pendant la création d'un texte, le texte saisi jusqu'alors est conservé, jusqu'à ce que vous quittiez la page. Dès que vous désactivez le bouton **Utiliser un texte personnalisé dans les rapports de quarantaine** et que vous enregistrez les modifications, tous les textes personnalisés dans toutes les langues sont perdus simultanément.

5. Créez un texte personnalisé dans la langue sélectionnée.

> **REMARQUE :**
>
> Il existe une limite de longueur de 800 caractères. Vous pouvez consulter la longueur actuelle sur un compteur sous le champ de saisie.

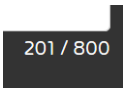


Illustration 329 : Nombre de caractères

6. Facultatif : Formatez votre texte selon vos envies. Vous pouvez ainsi utiliser des options de formatage du langage de balisage Markdown.

REMARQUE :

Les options de formatage suivantes sont prises en charge :

- Astérisque simple avec police italique : ***police italique***.
- Astérisque double pour caractères gras : ****caractères gras****.
- Un saut de ligne est représenté par une ligne vide. Sans cette ligne vide, le rapport de quarantaine se présenterait sur une seule ligne. Exemple :

  Voici un paragraphe. Voici un autre paragraphe.

- Une liste à puces peut être ajoutée en introduisant chaque élément de la liste comme une ligne séparée avec un tiret et un espace. Une ligne vide entre deux éléments de la liste est facultative et augmente l'espace entre les éléments de la liste. Toutefois, le premier élément de la liste doit être séparé du texte qui précède par une ligne vide. Le dernier élément de la liste doit également être séparé du texte qui suit au moyen d'une ligne vide. Exemple :

  - Premier élément de la liste

  - Deuxième élément de la liste

  - Troisième élément de la liste

- Les liens peuvent être ajoutés par des crochets autour du texte affiché et des parenthèses pour l'URL. Exemple :

  Cliquez [ici](https://une.url.tld).

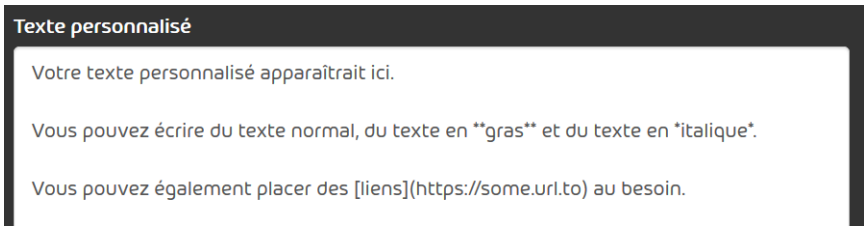


Illustration 330 : Exemple de texte dans le champ de saisie

7. Si vous avez terminé votre saisie dans toutes les langues souhaitées, enregistrez vos textes avec **Enregistrer**.

Vos textes personnalisés sont enregistrés et utilisés pour la prochaine distribution de rapports de quarantaine. La prévisualisation présente le résultat dans la langue actuellement sélectionnée une fois que vous avez cliqué sur **Enregistrer**.

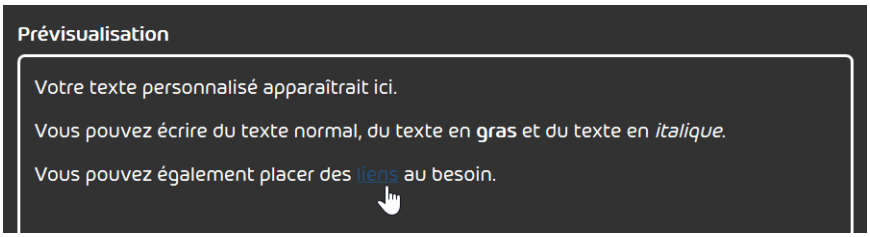


Illustration 331 : Exemple de texte dans le champ de prévisualisation

Des textes personnalisés ont été créés pour les rapports de quarantaine.

Désactiver le Quarantine Report pour un domaine

Vous avez activé le module **Quarantine Report** pour le domaine (voir Activer le Quarantine Report pour un domaine à la page 429).

Si les rapports de quarantaine ne doivent plus être générés pour les boîtes aux lettres d'un domaine, vous pouvez désactiver le module **Quarantine Report** (voir À propos du Quarantine Report à la page 418) pour ce domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez un domaine dans la sélection de l'espace.

3. Naviguez vers **Paramètres de sécurité** > **Quarantine Report**.
4. Actionnez le bouton **Activer Quarantine Report**.

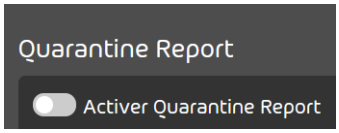


Illustration 332 : Désactiver le Quarantine Report

Le bouton devient gris.

Le module **Quarantine Report** a été désactivé pour une domaine.

Envoyer un courriel depuis le rapport de quarantaine

Vous avez activé le module **Quarantine Report** pour le domaine (voir Activer le Quarantine Report pour un domaine à la page 429).

Vous pouvez envoyer des courriels figurant dans les rapports de quarantaine (voir À propos du Quarantine Report à la page 418).

1. Ouvrez le rapport de quarantaine dans votre client de messagerie.
2. Dans le rapport de quarantaine, sélectionnez le courriel à envoyer.
3. Cliquez sur **Envoyer**.

Le courriel est remis au destinataire. Un avis d'envoi s'affiche dans le navigateur.

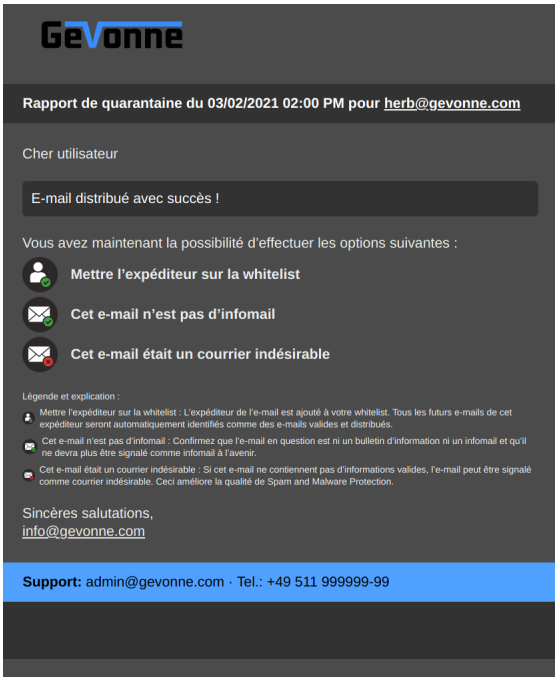


Illustration 333 : Avis d' envoi

REMARQUE :

Les rapports de quarantaine sont créés pour chacune des boîtes aux lettres principales. Si des boîtes aux lettres alias sont associées à une boîte aux lettres principale, les courriels destinés aux boîtes aux lettres alias sont répertoriés dans un rapport de quarantaine avec les courriels destinés à la boîte aux lettres principale. Lorsqu'un courriel provenant d'un rapport de quarantaine est envoyé, la boîte aux lettres à laquelle le courriel est adressé s'affiche en haut de la notification d'envoi.

4. Cliquez sur l'une des options avancées :
   - **Mettre l'expéditeur sur la whitelist** : l'expéditeur est autorisé pour l'utilisateur.
   - **Cet e-mail n'est pas d'infomail** : le courriel est classé comme **valide** à posteriori.
   - **Cet e-mail était un courrier indésirable** : le courriel est classé dans la catégorie des **spams** à posteriori s'il était auparavant classé dans la catégorie des infomails.

L'action sélectionnée est exécutée. Au lieu de l'avis d'envoi, une confirmation s'affiche dans le navigateur.

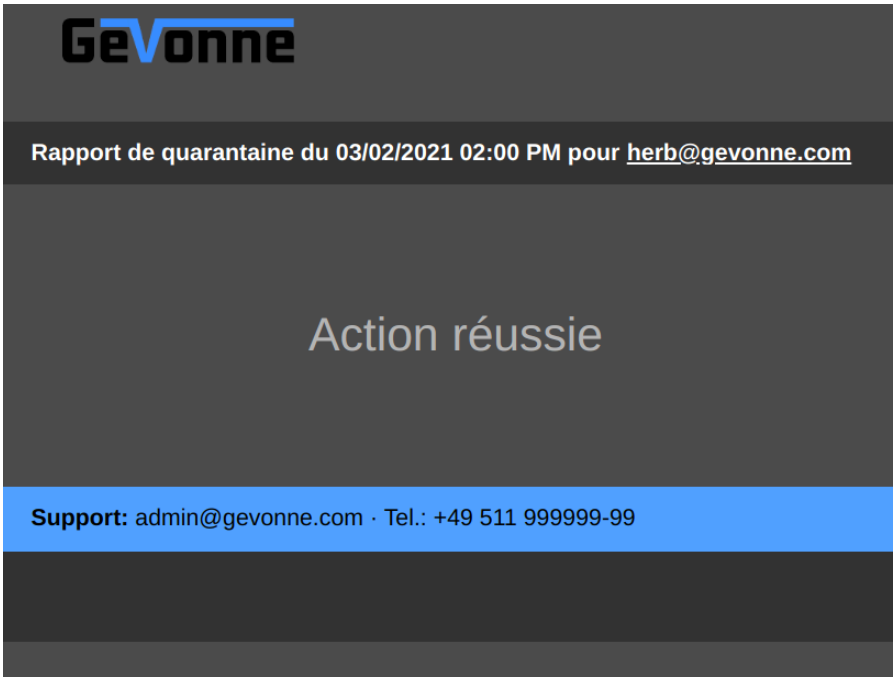


Illustration 334 : Fenêtre de confirmation

5. Fermez l'avis d'envoi.

Un courriel provenant d'un rapport de quarantaine a été envoyé.

Afficher la prévisualisation de courriel

Vous pouvez prévisualiser les courriels qui figurent dans les rapports de quarantaine (voir À propos du Quarantine Report à la page 418) et dont vous êtes le propriétaire. Pour plus d'informations

concernant la prévisualisation du courriel, voir le chapitre « Prévisualisation de courriel » dans le manuel du Control Panel.

1. Ouvrez le rapport de quarantaine dans votre client de messagerie.
2. Sélectionnez le courriel pour lequel vous souhaitez obtenir un aperçu.
3. Cliquez sur **Aperçu**.

Un aperçu simplifié du courriel s'affiche dans le navigateur.

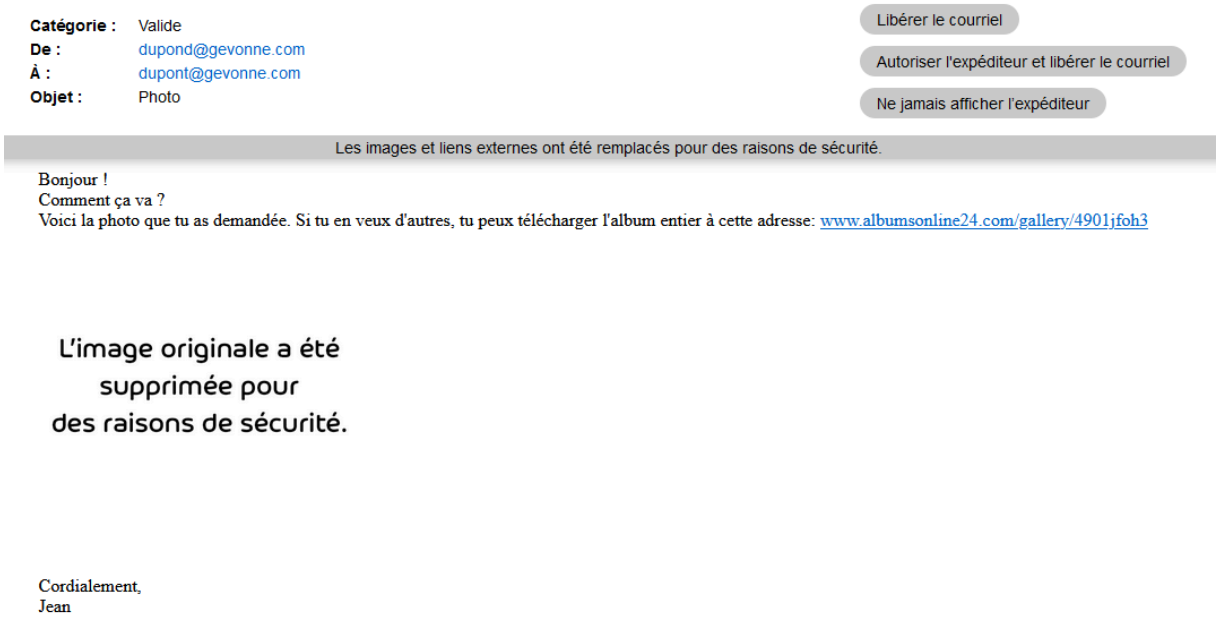


Illustration 335 : Prévisualisation de courriel

4. Fermer la prévisualisation de courriel.

Un aperçu a été affiché pour un courriel provenant d'un rapport de quarantaine.

Spam and Malware Protection

Spam and Malware Protection

Spam and Malware Protection est un service qui empêche les spams et les courriels qui contiennent des virus de parvenir dans la boîte aux lettres du destinataire. En outre, les infomails, tels que les newsletters, peuvent être reconnus et, en fonction des paramètres, distribués, mis en quarantaine ou marqués.

La Spam and Malware Protection offre une protection contre les menaces, les spams et les infomails grâce aux fonctions suivantes :

- Analyse des virus dans les courriels avec mise à jour automatique des signatures de virus et système d'alerte précoce pour les nouveaux virus et les virus inconnus jusqu'alors.
- Suivi des liens : les courriels entrants et sortants sont automatiquement vérifiés pour détecter les URL malveillantes.
- Détection des courriels de phishing : divers mécanismes, tels que le suivi des liens ou la détection des commandes de scripts malveillants, sont utilisés pour empêcher les tentatives de phishing.
- Filtrage en sortie : les courriels sortants sont contrôlés pour détecter les spams et les virus afin d'empêcher le client d'envoyer ou de transférer involontairement des logiciels malveillants et des spams.
- Gestion de rebonds : la Spam and Malware Protection rejette les notifications d'impossibilité de distribution qui arrivent en réponse à des spams dont les adresses d'expéditeurs ont été usurpées.

Les paramètres suivants concernant Spam and Malware Protection peuvent être configurés sous **Paramètres de sécurité** > **Spam and Malware Protection** :

- Activer la Spam and Malware Protection (voir Activer la Spam and Malware Protection à la page 453)
- Procéder à la configuration de l'environnement principal (voir Configuration d' environnement principal à la page 456)
- Configurer le traitement des spams et des infomails (voir Paramètres de filtre courriel à la page 462)

- Autoriser ou interdire les actions d'utilisateur (voir Autoriser ou interdire les actions d' utilisateur à la page 469)

Spam and Malware Protection permet à l'administrateur de déterminer lui-même comment traiter les spams et les infomails (voir Paramètres de filtre courriel à la page 462). En cas de faux positifs, les utilisateurs peuvent, en fonction des paramètres de l'administrateur, se faire envoyer des spams et des infomails via le **Email Live Tracking** (voir Actions sur les courriels à la page 89).

En outre, les services **Content Control** (voir À propos du Content Control à la page 472) et **Compliance Filter** (voir À propos du Compliance Filter à la page 487) sont inclus dans Spam and Malware Protection et peuvent être activés sur demande. L'ordre des règles (voir Ordre des règles dans tous les services à la page 451) indique l'ordre des filtres de tous les services.

Si le client ne souhaite plus utiliser la Spam and Malware Protection, il peut faire une demande au support technique pour désactiver ce service (voir Désactiver la Spam and Malware Protection à la page 470).

Ordre des règles dans tous les services

Les règles de la Spam and Malware Protection (voir « Spam and Malware Protection » dans le manuel du Control Panel) ont une certaine priorité dans laquelle elles sont traitées. Dès qu'une règle avec une priorité supérieure intervient, les règles avec une priorité inférieure ne sont plus traitées. Cela peut entraîner le blocage du courriel malgré l'entrée dans la liste des expéditeurs autorisés de l'adresse de l'expéditeur car l'adresse IPv4 du serveur expéditeur a été entrée sur la liste RBL des expéditeurs interdits.

Ordre des règles (priorité décroissante de haut en bas) :

Courriels entrants

1. Liste RBL (bloquer)
2. Détection de spams de masse (bloquer)
3. Compliance Filter
4. Email Authentication (bloquer)

5. Vérification de la présence de contenus malveillants (mettre en quarantaine)
6. Email Authentication (mettre en quarantaine)
7. Content Control, si activé (mettre en quarantaine)
8. Autorisation basée sur l'utilisateur (distribuer)
9. Interdiction basée sur l'utilisateur (mettre en quarantaine)
10. Autorisation administrative (distribuer)

> **REMARQUE :**
>
> La création administrative d'expéditeurs autorisés est un cas particulier parmi les règles. En effet, les administrateurs peuvent choisir, pour les entrées d'expéditeurs autorisés au niveau d'un domaine, quels filtres seront contournés par l'entrée (voir « Créer une entrée d'expéditeur interdit pour un domaine » dans le manuel du Control Panel). Les courriels concernés sautent donc les filtres sélectionnés lorsqu'ils sont traités. Cela vaut également pour les filtres qui se trouvent dans la liste avant les expéditeurs autorisés administratifs. La position à laquelle les expéditeurs autorisés administratifs sont classés dans la liste fait référence au réglage par défaut des entrées des expéditeurs autorisés au niveau d'un domaine. Par défaut, les entrées contournent le filtrage du spam comme un seul filtre.

11. Interdiction administrative (mettre en quarantaine)
12. Autorisation générale (distribuer)
13. Règles générales de spam (mettre en quarantaine)
14. Filtre infomail (mettre en quarantaine)

REMARQUE :

Le Compliance Filter (voir À propos du Compliance Filter à la page 487) est appliqué avant le Content Control (voir À propos du Content Control à la page 472). Par conséquent, les administrateurs peuvent créer des exceptions au Content Control avec des règles du Compliance Filter qui classent les courriels dans la catégorie **Valide**.

Pour le Content Control en revanche, il n'est pas possible de créer des exceptions via les expéditeurs autorisés et les expéditeurs interdits définis par l'utilisateur, ni via les expéditeurs interdits administratifs, car ces règles ne sont appliquées qu'après le Content Control. Seule la création administrative d'expéditeurs autorisés permet de contourner le Content Control.

Courriels sortants

1. Liste RBL
2. Compliance Filter
3. Vérification de la présence de contenus malveillants
4. Content Control, si activé

Activer la Spam and Malware Protection

Dans le module **Paramètres de sécurité** > **Spam and Malware Protection**, vous pouvez désactiver Spam and Malware Protection (voir Spam and Malware Protection à la page 450) pour un domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer la Spam and Malware Protection.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.

4. Sous **Domaine**, sélectionnez le domaine pour lequel vous souhaitez activer la Spam and Malware Protection.

Illustration 336 : Sélectionner un domaine

> **REMARQUE :**
>
> La Spam and Malware Protection ne peut être définie pour les domaines alias que si elle est activée pour le domaine principal associé. Par défaut, les paramètres du domaine principal sont hérités par les domaines alias.

5. Actionnez le bouton **Activer Spam and Malware Protection** sous **Paramètres de l'environnement primaire**.

Illustration 337 : Activer la Spam and Malware Protection

Une fenêtre de confirmation apparaît.

6. **ATTENTION :**

   Dès que la Spam and Malware Protection est activée, une période d'essai gratuite de 30 jours démarre. Une fois la période d'essai terminée, le service devient payant.

   IMPORTANT :

   Les administrateurs ne peuvent pas désactiver l'Spam and Malware Protection eux-mêmes. Seul le support technique peut désactiver Spam and Malware Protection.

   Cliquez sur **Confirmer**.

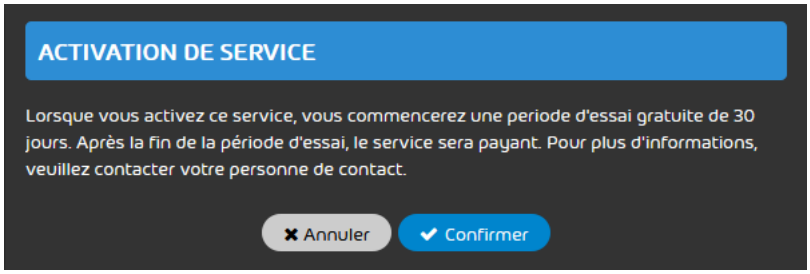


Illustration 338 : Confirmer

Le bouton devient vert et des commandes supplémentaires sont activées sous **Paramètres de l'environnement primaire** et **Paramètres de filtre e-mail**.

7. Facultatif : Si vous souhaitez modifier les paramètres d'environnement et les paramètres de filtre de courriel avant que Spam and Malware Protection ne soit actif, modifiez les paramètres maintenant (voir Procéder à la configuration de l' environnement principal à la page 457 et Paramètres de filtre courriel à la page 462).
8. Cliquez sur **Enregistrer**.

Spam and Malware Protection a été activé pour le domaine.

Vous pouvez ensuite effectuer des réglages dans votre environnement principal (voir Configuration d' environnement principal à la page 456) et configurer les paramètres de filtre courriel (voir Paramètres de filtre courriel à la page 462).

Configuration d’ environnement principal

La configuration d'environnement principal pour le domaine client est gérée dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450).

La Spam and Malware Protection nécessite une configuration d'environnement principal spécifique pour la réception et l'envoi de courriels. Sous **Paramètres de l'environnement primaire**, les administrateurs côté clients peuvent spécifier la destination des courriels entrants, définir des adresses IPv4 pour les serveurs de relais divergents, activer la gestion de rebonds et définir la vérification d'utilisateurs.

Pour une meilleure compréhension, voici une brève explication des options disponibles. Pour de plus amples informations sur la configuration, voir Procéder à la configuration de l’ environnement principal à la page 457.

- **Destination** : Sous **Destination**, la destination des courriels entrants à traiter par la Spam and Malware Protection est saisie. Les options disponibles sont les suivantes :
  - **IP/nom d'hôte** : il s'agit du cas standard. Les serveurs de messagerie du client sont ici référencés en spécifiant soit les adresses IPv4 correspondantes, soit les noms d'hôtes correspondants. Lorsqu'un nom d'hôte est spécifié, une résolution enregistrement MX est effectuée en premier, suivie d'une résolution enregistrement A.
- **Adresses IP de serveurs de relais pour les courriels sortants** : Si la Spam and Malware Protection est activée, les courriels sortants sont également filtrés. Par conséquent, les adresses IPv4 des serveurs de relais pour les courriels du client à partir desquels les courriels sortants sont envoyés à nos serveurs peuvent être saisies sous **Adresses IP de serveurs de relais pour les courriels sortants**, de sorte que la Spam and Malware Protection puisse vérifier si un courriel provient effectivement du client.

  Plusieurs adresses de serveurs de relais séparées par des virgules avec des suffixes de maximum /24 peuvent être saisies ici. Il existe une limite de caractère de 65 535 caractères. Il est également possible d'entrer des plages CIDR. Si un courriel est envoyé via l'une des adresses IP saisies, la Spam and Malware Protection intervient. Si cette option n'est pas activée, tous

les courriels sortants provenant d'adresses courriel du domaine seront filtrés par la Spam and Malware Protection.

> **IMPORTANT :**
>
> Les adresses de serveurs de relais saisies ici sont également nécessaires pour la signature et le cryptage des courriels dans le cadre de Signature and Disclaimer. Si aucune adresse n'est saisie, aucun courriel ne peut être traité par ces deux services. Même si ces services ne sont pas utilisés, nous recommandons aux administrateurs côté clients de saisir ici leurs adresses de serveurs de relais.

- **Restreindre l'envoi de courriels aux adresses IP des serveurs de relais** : Ce paramètre garantit que les courriels sortants des adresses courriel du domaine soient envoyés uniquement via notre infrastructure s'ils ont été envoyés depuis l'une des adresses des serveurs de relais saisies.
- **Gestion de rebonds (recommandée)** : La gestion de rebonds est une fonction qui, en cas de notifications d'impossibilité de distribution entrantes, vérifie si les courriels en cause ont été effectivement envoyés via les serveurs de messagerie de relais du domaine ou via une fausse adresse d'expéditeur comme un retour d'une attaque de spam. Dans le second cas, les notifications d'impossibilité de distribution sont refusées.
- **Vérification d'utilisateurs** : Lors de la vérification d'utilisateurs, la Spam and Malware Protection vérifie les courriels entrants pour voir si les adresses des destinataires existent. Si l'adresse du destinataire d'un courriel n'existe pas, la Spam and Malware Protection rejettera le courriel. Cela empêche nos serveurs de messagerie d'accepter des courriels à des adresses inexistantes sous les domaines de nos clients, qui pourraient être exploitées contre nos clients pour des attaques DDOS. La vérification d'utilisateurs peut être effectuée sur la base de la population d'utilisateurs dans le Control Panel ou directement via une requête SMTP aux serveurs de messagerie du domaine d'un client qui sont entrés sous **Destination**.

Procéder à la configuration de l'environnement principal

Vous avez activé la Spam and Malware Protection.

La Spam and Malware Protection (voir Spam and Malware Protection à la page 450) nécessite une configuration de l'environnement primaire pour la réception et l'envoi de courriels. Sous

Configuration d'environnement principal à la page 456, vous trouverez des informations plus détaillées sur les fonctions.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez procéder à la configuration de l'environnement primaire.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Dans **Domaine**, sélectionnez le domaine pour lequel vous souhaitez procéder à la configuration de l'environnement primaire.
5. Facultatif : Si vous avez sélectionné un domaine alias, qui reprend jusqu'à présent les paramètres du domaine principal, actionnez le bouton **Reprendre du domaine primaire**.

Le bouton devient gris. Les paramètres du module sont activés.

6. Dans **Destination**, définissez le serveur de destination des courriels entrants. Il existe les possibilités suivantes :

   - Si vous disposez de votre propre serveur de messagerie, cochez la case **IP/nom d'hôte**, puis saisissez l'adresse IPv4 ou le nom d'hôte du serveur de destination dans le champ. Saisissez au moins une adresse IPv4 ou un nom d'hôte. En option, vous pouvez également spécifier le numéro de port et la priorité. Respectez le format de saisie **IPv4/nom d'hôte:Port#Priorité** et utilisez un point-virgule pour séparer les entrées multiples.
   -
   -

REMARQUE :

Ce serveur de destination est désigné dans le Control Panel comme l'environnement primaire. Par défaut, le trafic de courriels entrants des boîtes aux lettres du domaine est dirigé à l'environnement primaire. Pour diriger le trafic de courriels entrants d'une boîte aux lettres distincte vers un autre serveur de destination, un environnement secondaire (voir « Environnements secondaires » dans le manuel du Control Panel) peut être attribué à la boîte aux lettres à la place de l'environnement primaire (voir Modifier l'environnement à la page 257).

7. **REMARQUE :**

   , cette étape est facultative mais fortement recommandée. Les adresses saisies sous **Adresses IP de serveurs de relais pour les courriels sortants** sont nécessaires pour la signature de courriels dans le cadre de Signature and Disclaimer. Si aucune adresse n'est saisie, aucun courriel ne peut être traité par ces deux services.

   Facultatif : Si vous souhaitez saisir manuellement les adresses IP de vos serveurs de relais, cliquez sur le bouton **Adresses IP de serveurs de relais pour les courriels sortants**.

   Un champ pour la saisie des adresses IPv4 s'affiche.

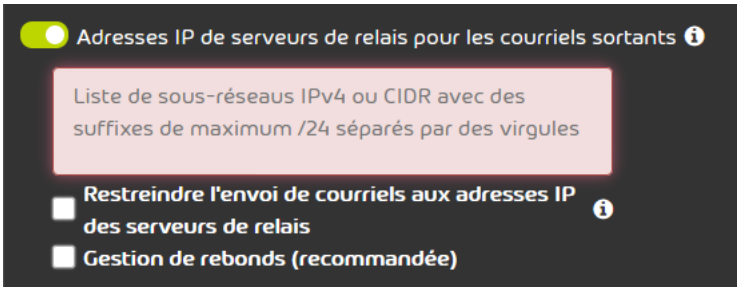


Illustration 339 : Définir les adresses IP des serveurs de relais pour les courriels sortants

8. Facultatif : Saisissez les adresses IPv4 de vos smarthosts dans le champ situé sous le bouton **Adresses IP de serveurs de relais pour les courriels sortants**. Si le bouton est activé, ce champ ne doit pas être laissé vide.

   REMARQUE :

   Plusieurs adresses IPv4 de smarthosts séparées par des virgules avec des suffixes de maximum /24 peuvent être saisies ici. Ce champ peut contenir un maximum de 65 535 caractères.

9. Facultatif : Pour vous assurer que les courriels sortants du domaine sont envoyés exclusivement via les adresses IP de serveurs relais saisies, cochez la case **Restreindre l'envoi de courriels aux adresses IP des serveurs de relais**.

> **REMARQUE :**
>
> Ce paramètre est activé par défaut. Ce paramètre garantit que les courriels sortants des adresses courriel du domaine sont envoyés via notre infrastructure uniquement s'ils ont été envoyés par l'une des adresses IPv4 de smarthosts saisies.

10. Facultatif : Si vous souhaitez activer la gestion de rebonds pour éviter les notifications d'impossibilité de distribution inappropriées, cochez la case **Gestion de rebonds (recommandée)**.

11.

> **REMARQUE :**
>
> Cette étape est possible uniquement pour les clients qui ont sélectionné **IP/nom d'hôte** comme cible pour leur environnement primaire.

Facultatif : Configurez la vérification d'utilisateurs dans la section **Vérification d'utilisateurs**. Vous avez les options suivantes :

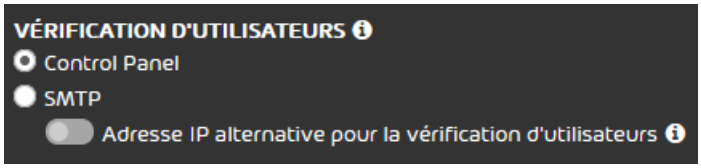


Illustration 340 : Configurer la vérification d' utilisateurs

- **Control Panel** : si vous cochez cette case, la Spam and Malware Protection vérifie si l'adresse du destinataire figure dans la liste des utilisateurs du Control Panel. Ce paramètre

empêche la création automatique de boîtes aux lettres dans le Control Panel (voir Boîtes aux lettres à la page 213).

> **REMARQUE :**
>
> Si cette option est sélectionnée, toutes les boîtes aux lettres souhaitées et leurs adresses alias doivent être présentes dans le Control Panel. Les boîtes aux lettres peuvent être ajoutées au Control Panel manuellement ou être synchronisées avec un service d'annuaire via LDAP .

- **SMTP** : si vous cochez cette case, la Spam and Malware Protection vérifie l'adresse du destinataire par un rappel SMTP. Pour ce faire, la Spam and Malware Protection demande au serveur de destination de l'adresse du destinataire si celle-ci est valide. Par défaut, le serveur de destination est déterminé via la partie domaine. Si vous souhaitez utiliser un serveur de destination différent pour la vérification d'utilisateurs avec SMTP, actionnez le bouton **Adresse IP alternative pour la vérification d'utilisateurs** et saisissez l'adresse IPv4 dans le champ de saisie. Vous pouvez saisir un sous-réseau IPv4 ou CIDR.

> **REMARQUE :**
>
> Si la vérification des utilisateurs entraîne des problèmes, veuillez contacter le support.

12. Cliquez sur **Enregistrer**.

Si l'option **SMTP** a été sélectionnée pour la vérification d'utilisateurs, un message d'avertissement apparaît. Si ce n'est pas le cas, les paramètres sont enregistrés.

13. Si l'option **SMTP** a été sélectionnée pour la vérification d'utilisateurs, cliquez sur **Confirmer**.

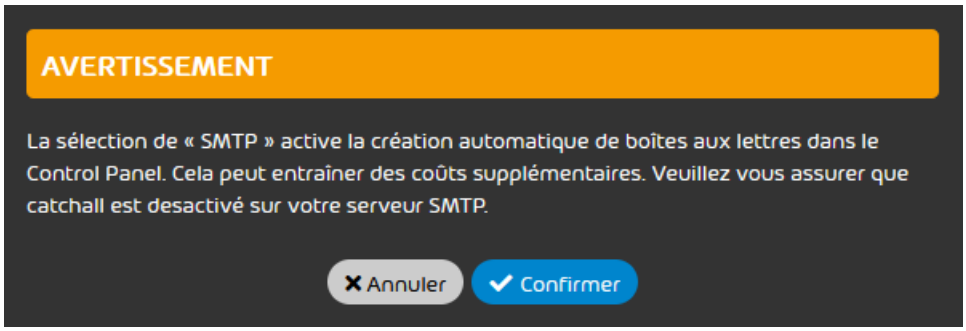


Illustration 341 : Confirmer

Les paramètres sont mémorisés.

Les paramètres de l'environnement primaire de la Spam and Malware Protection ont été définis.

Vous pouvez ensuite modifier les paramètres de filtre courriel (voir Paramètres de filtre courriel à la page 462) ou autoriser ou interdire les actions d'utilisateur (voir Autoriser ou interdire les actions d' utilisateur à la page 469).

Paramètres de filtre courriel

Dans la section **Paramètres de filtre e-mail** du module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450), les administrateurs côté clients peuvent configurer divers paramètres pour le filtre courriel.

Sous **Paramètres de sécurité** > **Spam and Malware Protection** > **Paramètres de filtre e-mail**, les administrateurs côté clients ont les options suivantes :

- Configurer la gestion de spams (voir Configurer la gestion de spams à la page 463).
- Activer le filtre infomail (voir Activer le filtre infomail à la page 465).
- Configurer le filtre infomail (voir Configurer le filtre infomail à la page 465).
- Configurer la gestion des infomails (voir Configurer la gestion des infomails à la page 467).

Configurer la gestion de spams

Vous avez activé la **Spam and Malware Protection** (voir Activer la Spam and Malware Protection à la page 453).

Sous **Gestion de spams** dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450), vous pouvez décider de ce qu'il faut faire des spams interceptés par le filtre courriel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez configurer la gestion de spams.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Dans **Domaine**, sélectionnez le domaine pour lequel vous souhaitez configurer la gestion de spams.
5. Facultatif : Si vous avez sélectionné un domaine alias, qui reprend jusqu'à présent les paramètres du domaine principal, appuyez sur le bouton **Reprendre du domaine primaire**.

Le bouton devient gris. Les paramètres du module sont activés.

6. Sélectionnez l'option souhaitée pour la gestion de spams sous **Paramètres de filtre e-mail** > **Gestion de spams**. Vous avez deux options :

   - Si vous souhaitez enregistrer les spams en quarantaine, sélectionnez **Enregistrer en quarantaine**. Pour les courriels mis en quarantaine, le module **Email Live Tracking** propose différentes actions.
   - Si vous souhaitez marquer les spams par un ajout personnalisé, sélectionnez **Marquer**. Le champ de saisie **Phrase pour le marquage** est alors affiché. Saisissez-y l'ajout avec lequel les spams doivent être marqués.

Illustration 342 : Marquer les spams

> **REMARQUE :**
>
> Les courriels de la catégorie **Spam** ne sont mentionnés dans les rapports de quarantaine (voir le chapitre « À propos du Quarantine Report » dans le manuel du Control Panel) que s'ils ont été mis en quarantaine et que la catégorie de courriel est sélectionnée pour être affichée dans les rapports de quarantaine (voir le chapitre « Configurer le Quarantine Report pour un domaine » dans le manuel du Control Panel).

7. Cliquez sur **Enregistrer**.

La gestion de spams a été interrompue.

Vous pouvez ensuite activer le filtre infomail (voir Activer le filtre infomail à la page 465), ou autoriser ou interdire les actions d'utilisateur (voir Autoriser ou interdire les actions d' utilisateur à la page 469).

Activer le filtre infomail

Vous avez activé **Spam and Malware Protection** (voir Activer la Spam and Malware Protection à la page 453).

Sous **Gestion d'infomails** dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450), vous pouvez activer le filtre infomail pour un domaine principal et régler d'autres paramètres. Les paramètres valent également pour les domaines alias du domaine principal.

Le filtre infomail reconnaît les infomails et effectue diverses actions en fonction des paramètres. Le filtre infomail fait partie de la fonctionnalité du filtre courriel de **Spam and Malware Protection**. Pour utiliser le filtre infomail, vous devez d'abord l'activer.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer le filtre infomail.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Dans **Domaine**, sélectionnez le domaine principal pour lequel vous souhaitez activer le filtre infomail.
5. Actionnez le bouton **Activer le filtre infomail**.

   Le bouton devient vert et un formulaire avec d'autres paramètres s'affiche.
6. Cliquez sur **Enregistrer**.

Le filtre infomail a été activé pour un domaine principal et ses domaines alias.

Vous pouvez ensuite définir le filtre infomail (voir Configurer le filtre infomail à la page 465).

Configurer le filtre infomail

Vous avez activé la **Spam and Malware Protection** et le filtre infomail (voir Activer la Spam and Malware Protection à la page 453 et Activer le filtre infomail à la page 465).

Sous **Gestion d'infomails** dans le module **Spam and Malware Protection** (voir « Spam and Malware Protection » dans le manuel du Control Panel), vous pouvez configurer le filtre infomail afin

de régler sa portée pour un client. Les paramètres sont valables aussi bien pour le domaine principal que pour les domaines alias du client.

Vous pouvez activer ou désactiver le filtre infomail par défaut pour tous les utilisateurs du client. Vous pouvez également définir si les utilisateurs peuvent activer ou désactiver le filtre infomail pour leur propre boîte aux lettres (voir « Configurer les rapports de quarantaine » dans le manuel du Control Panel). Les utilisateurs peuvent ainsi décider eux-mêmes s'ils souhaitent utiliser le filtre infomail.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez régler le filtre infomail.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Sous **Domaine**, sélectionnez le domaine principal pour lequel vous souhaitez paramétrer le filtre infomail.
5. Si vous souhaitez activer le filtre infomail par défaut pour tous les utilisateurs du client, cochez la case **Activer le filtre infomail pour tous les utilisateurs** sous **Paramètres de filtre e-mail** > **Gestion d'infomails**.
6. Si vous souhaitez autoriser les utilisateurs du client à activer et à désactiver le filtre infomail, cochez la case **Permettre aux utilisateurs d'activer et de désactiver le filtre infomail**. Si la case est cochée, les utilisateurs peuvent activer et désactiver le filtre infomail sous **Paramètres utilisateur** > **Filtres & rapports** (voir « Configurer les rapports de quarantaine » dans le manuel du Control Panel). Les options suivantes résultent de la combinaison des deux cases à cocher :

   - **Permettre aux utilisateurs d'activer et de désactiver le filtre infomail** activé, désactivé : le filtre infomail est activé pour tous les utilisateurs. Les utilisateurs ne peuvent pas désactiver le filtre infomail.
   - **Permettre aux utilisateurs d'activer et de désactiver le filtre infomail** activé, activé : le filtre infomail est activé par défaut pour tous les utilisateurs. Les utilisateurs peuvent désactiver le filtre infomail.
   - **Permettre aux utilisateurs d'activer et de désactiver le filtre infomail** désactivé, activé : le filtre infomail est désactivé par défaut pour tous les utilisateurs. Les utilisateurs peuvent activer le filtre infomail.

- **Permettre aux utilisateurs d'activer et de désactiver le filtre infomail** désactivé, désactivé : le filtre infomail est désactivé pour tous les utilisateurs. Les utilisateurs ne peuvent pas activer le filtre infomail. Une fois que vous avez appliqué les modifications, le bouton **Activer le filtre infomail** est grisé et les paramètres avancés sont masqués.

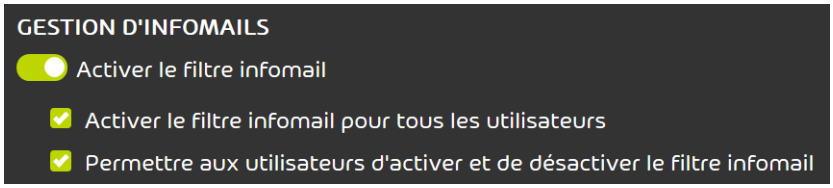


Illustration 343 : Configurer le filtre infomail

7. Cliquez sur **Enregistrer**.

Le filtre infomail a été configuré.

Vous pouvez ensuite configurer la gestion des infomails (voir Configurer la gestion des infomails à la page 467) ou autoriser ou interdire les actions d'utilisateur (voir Autoriser ou interdire les actions d' utilisateur à la page 469).

Configurer la gestion des infomails

Vous avez activé la **Spam and Malware Protection** et le filtre infomail (voir Activer la Spam and Malware Protection à la page 453 et Activer le filtre infomail à la page 465).

Sous **Gestion d'infomails** dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450), vous pouvez décider de ce qu'il faut faire des infomails interceptés par le filtre courriel.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez configurer la gestion des infomails.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Dans **Domaine**, sélectionnez le domaine pour lequel vous souhaitez configurer la gestion des infomails.

5. Facultatif : Si vous avez sélectionné un domaine alias, qui reprend jusqu'à présent les paramètres du domaine principal, appuyez sur le bouton **Reprendre du domaine primaire**.
6. Sélectionnez l'option souhaitée pour la gestion des infomails sous **Paramètres de filtre e-mail** > **Gestion d'infomails**. Vous avez deux options :
   - Si vous souhaitez enregistrer les infomails en quarantaine, sélectionnez **Enregistrer en quarantaine**. Pour les courriels mis en quarantaine, le module **Email Live Tracking** (voir Email Live Tracking à la page 59) propose différentes actions (voir Actions sur les courriels à la page 89).
   - Si vous souhaitez marquer les infomails par un ajout personnalisé, sélectionnez **Marquer**. Le champ de saisie **Phrase pour le marquage** est alors affiché. Saisissez-y l'ajout avec lequel les infomails doivent être marqués.

Illustration 344 : Marquer les infomails

> **REMARQUE :**
>
> Tous les courriels classés comme **Infomail** sont répertoriés dans les rapports de quarantaine quel que soit ce paramètre. Cette mesure s'applique uniquement si vous avez activé le filtre d'infomail et si vous avez sélectionné la catégorie **Infomail** dans le rapport de quarantaine pour qu'elle s'affiche (voir Configurer le Quarantine Report pour un domaine à la page 430).

7. Cliquez sur **Enregistrer**.

La gestion des infomails a été interrompue.

Vous pouvez ensuite autoriser ou interdire les actions d'utilisateur (voir Autoriser ou interdire les actions d' utilisateur à la page 469).

Autoriser ou interdire les actions d'utilisateur

Sous **Droits d'utilisateurs** dans le module **Spam and Malware Protection** (voir Spam and Malware Protection à la page 450), vous pouvez autoriser ou interdire aux utilisateurs de votre domaine d'effectuer des actions avec les courriels interceptés par la Spam and Malware Protection.

Dans le module **Email Live Tracking** (voir Email Live Tracking à la page 59) et dans les rapports de quarantaine (voir À propos du Quarantine Report à la page 418), les utilisateurs disposent d'actions pour se faire livrer leurs propres courriels qui ont été interceptés par la Spam and Malware Protection. Vous pouvez autoriser ou interdire les actions. Les administrateurs côté clients ont l'autorisation, quels que soient les paramètres, d'envoyer tous les courriels depuis le module **Email Live Tracking**.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez un domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Spam and Malware Protection**.
4. Sélectionnez l'onglet **Droits d'utilisateurs**.

L'onglet **Droits d'utilisateurs** s'ouvre.

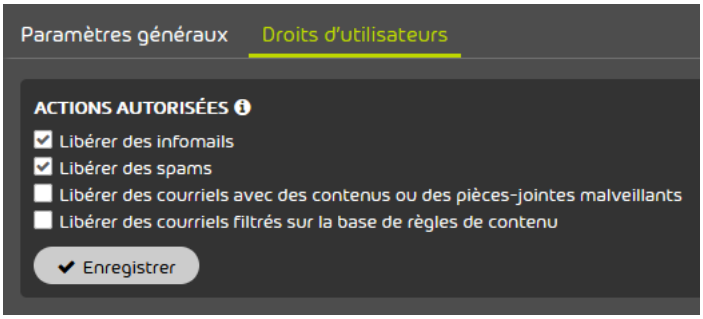


Illustration 345 : Droits d'utilisateur

5. Sous **Actions autorisées**, cochez les cases des actions que vous souhaitez autoriser aux utilisateurs du domaine. Désactivez les cases à cocher des actions que vous souhaitez interdire aux utilisateurs du domaine. Les actions suivantes sont disponibles :

   - **Libérer des infomails**.
   - **Libérer des spams**.
   - **Envoyer des e-mails avec des pièces-jointes malveillantes**.
   - **Libérer des courriels filtrés sur la base de règles de contenu**.

   > **REMARQUE :**
   >
   > Les utilisateurs ne peuvent envoyer aucun courriel de la catégorie **AdvThreat**, quels que soient les paramètres. Seuls les administrateurs et les utilisateurs avec le rôle **Service Desk** peuvent envoyer des courriels de cette catégorie.

6. Cliquez sur **Enregistrer**.

Les actions d'utilisateur avec les courriels interceptés par la Spam and Malware Protection ont été autorisées ou interdites.

Vous pouvez ensuite activer le filtre infomail (voir Activer le filtre infomail à la page 465).

Désactiver la Spam and Malware Protection

Vous avez activé la Spam and Malware Protection (voir Spam and Malware Protection à la page 450) pour un domaine principal. Vous avez modifié les enregistrements MX dans la zone DNS de votre domaine pour les ramener à votre serveur de messagerie.

Si vous ne souhaitez plus utiliser la Spam and Malware Protection, vous pouvez faire désactiver le service par le support technique. Les paramètres sont conservés au cas où vous voudriez réactiver la Spam and Malware Protection ultérieurement.

AVERTISSEMENT :

Si la Spam and Malware Protection est désactivée et que les enregistrements MX de la zone DNS de votre domaine n'ont pas été basculés au préalable vers votre serveur de messagerie, vos courriels entrants ne seront pas transférés vers votre serveur de messagerie et risquent d'être perdus.

Avant de désactiver la Spam and Malware Protection, assurez-vous que les enregistrements MX de la zone DNS de votre domaine pointent vers votre serveur de messagerie.

DANGER :

Une fois la Spam and Malware Protection désactivée, les services suivants ne peuvent plus être utilisés, même s'ils apparaissent comme étant activés dans le Control Panel :

- Advanced Threat Protection (voir Structure et fonction d' ATP à la page 357)
- Compliance Filter (voir À propos du Compliance Filter à la page 487)
- Content Control (voir À propos du Content Control à la page 472)
- Continuity Service (voir À propos du Continuity Service à la page 603)
- Email Authentication (voir À propos de l' Email Authentication à la page 382)
- Quarantine Report (voir À propos du Quarantine Report à la page 418)

IMPORTANT :

Une fois que la Spam and Malware Protection est désactivée pour le domaine principal, les paramètres du service ne peuvent pas être modifiés pour les domaines alias. Par conséquent, assurez-vous que la Spam and Malware Protection est correctement configurée pour les domaines alias avant de désactiver le service pour le domaine principal.

Indiquez au support technique ou à votre interlocuteur que vous souhaitez désactiver la Spam and Malware Protection pour le domaine principal ou un domaine alias.

L'assistance traitera la demande de désactivation.

IMPORTANT :

La désactivation de la Spam and Malware Protection n'entraîne pas la résiliation du contrat existant pour ce service. Pour annuler un contrat existant, vous devez contacter votre interlocuteur.

Spam and Malware Protection a été désactivée.

Content Control

À propos du Content Control

Avec le Content Control, les administrateurs côté clients peuvent gérer le traitement des pièces jointes des courriels entrants et sortants.

Avant que Content Control ne puisse être utilisé, un administrateur côté clients doit activer Content Control (voir Activer le Content Control à la page 474). Les administrateurs côté clients pourront ensuite configurer Content Control (voir Configurer le Content Control à la page 477).

Les administrateurs côté clients peuvent définir une taille maximale autorisée pour les courriels. Les courriels qui dépassent cette taille seront filtrés. En outre, les administrateurs peuvent décider quels types de pièces jointes doivent être filtrés. Les types de pièces-jointes suivants sont disponibles :

- Pièces-jointes cryptées
- Pièces-jointes exécutables
- Données Office avec macros

Les administrateurs peuvent également interdire des types de fichiers en fonction de leur extension. Les types de fichiers interdits peuvent être définis aussi bien pour les fichiers directement en pièce-jointe que pour les fichiers qui figurent dans les archives. En outre, des mots-clés collectifs (voir Vue d'ensemble des mots-clés collectifs à la page 473) permettent d'interdire plusieurs types de fichiers à la fois.

Les administrateurs côté clients peuvent décider si les courriels filtrés sont mis en quarantaine ou si les courriels sont envoyés sans pièces-jointes aux destinataires. Dans le deuxième cas, les destinataires sont informés que les pièces-jointes ont été séparées.

Les paramètres peuvent être configurés soit pour toutes les boîtes aux lettres d'un domaine, soit pour des groupes de boîtes aux lettres (voir « Groupes » dans le manuel du Control Panel). Pour configurer les paramètres d'un groupe, celui-ci doit être ajouté à Content Control (voir Ajouter un groupe au Content Control à la page 475). Les groupes sont classés dans Content Control en fonction de leur priorité et traités dans cet ordre. Si une boîte aux lettres appartient à plusieurs groupes, les paramètres du groupe avec la priorité la plus élevée seront appliqués à la boîte aux lettres. Les administrateurs peuvent modifier les priorités des groupes (voir Modifier les priorités des groupes à la page 483). Si les paramètres généraux du domaine doivent à nouveau s'appliquer aux boîtes aux lettres d'un groupe , les administrateurs peuvent supprimer le groupe de Content Control (voir Supprimer un groupe de Content Control à la page 485).

Vue d' ensemble des mots-clés collectifs

Le tableau suivant présente les mots-clés collectifs que les administrateurs côté clients peuvent utiliser pour filtrer des groupes de types de fichiers dans les pièces jointes avec Content Control (voir À propos du Content Control à la page 472).

MOT-CLÉ COLLECTIF	TYPES DE FICHIERS FILTRÉS
.executable	.action .apk .app .bas .bat .bin .cab .chm .cmd .com .command .cpl .csh .dll .exe .gadget .hta .inf .ins .inx .ipa .isu .job .jar .js .jse .ksh .lnk .msc .msi .msp .mst .osx .paf .pcd .pif .prg .ps1 .reg .rgs .run .scr .sct .sh .shb .shs .u3p .vb .vba .vbe .vbs .vbscript. vbx .workflow .ws .wsc .wsf .wsh
.mediafile	.aif .flv .mp1 .mid .mp5 .mpa .wma .mp2 .mpe .swf .wmf .wav .mp4 .wmv .mpg .avi .mov .mp3 .mpv2 .mp2v .aiff .mpeg
.docmacro	Fichiers Microsoft Word avec macros. Les fichiers Microsoft Word en pièce jointe sont

MOT-CLÉ COLLECTIF	TYPES DE FICHIERS FILTRÉS
	analysés à l'aide d'une détection heuristique des modèles de macro. Ce filtre ne couvre pas tous les types de macros.
.xlsmacro	Fichiers Microsoft Excel avec macros. Les fichiers Microsoft Excel en pièce jointe sont analysés à l'aide d'une détection heuristique des modèles de macro. Ce filtre ne couvre pas tous les types de macros.
.pptmacro	Fichiers Microsoft PowerPoint avec macros. Les fichiers Microsoft PowerPoint en pièce jointe sont analysés à l'aide d'une détection heuristique des modèles de macro. Ce filtre ne couvre pas tous les types de macros.

Activer le Content Control

Vous avez activé la Spam and Malware Protection (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Dans le module **Paramètres de sécurité** > **Content Control**, vous pouvez activer le Content Control (voir À propos du Content Control à la page 472) pour gérer le traitement des pièces jointes des courriels entrants et sortants pour les utilisateurs d'un domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.

4. Actionnez le bouton **Activer Content Control**.

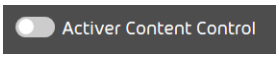


Illustration 346 : Activer le Content Control

Le bouton devient vert.

Le Content Control a été activé pour le domaine sélectionné. Les paramètres par défaut du Content Control sont appliqués à tous les utilisateurs sous le domaine.

Vous pouvez ensuite définir les paramètres par défaut du Content Control pour le domaine (voir Configurer le Content Control à la page 477). Si vous souhaitez définir des paramètres pour des groupes, vous devez d'abord ajouter des groupes au Content Control (voir Ajouter un groupe au Content Control à la page 475). Si vous ne souhaitez plus utiliser le Content Control, vous pouvez désactivez le Content Control (voir Désactiver le Content Control à la page 486).

Ajouter un groupe au Content Control

Vous avez activé le Content Control (voir Activer le Content Control à la page 474). Vous avez créé un groupe sous le domaine (voir « Créer un groupe » dans le manuel du Control Panel).

Les paramètres dans le module **Content Control** s'appliquent par défaut à tous les utilisateurs d'un domaine. Sous **Paramètres de sécurité** > **Content Control**, vous pouvez toutefois ajouter des groupes au Content Control pour configurer le Content Control pour ces groupes différemment des autres utilisateurs du domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez ajouter un groupe au Content Control.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.

4. Cliquez sur le menu déroulant sous **Groupes concernés**.

Illustration 347 : Sélectionner un groupe

- Le menu déroulant s'ouvre. Le menu déroulant contient les groupes du domaine.

5. Dans le menu déroulant, sélectionnez le groupe que vous souhaitez ajouter au Content Control.
6. Cliquez sur **Ajouter**.

- Le groupe est ajouté à la liste de groupes ci-dessous. Le groupe est placé à la fin de la liste.

> **REMARQUE :**
>
> Les groupes sont classés en fonction de leur priorité. Les priorités sont indiquées dans la colonne **Priorité**. Plus le nombre est bas, plus un groupe est prioritaire. Les règles du groupe avec la priorité la plus élevée sont appliquées à une boîte aux lettres qui appartient à plusieurs groupes dans le module **Content Control**. Les priorités des groupes peuvent être modifiées (voir Modifier les priorités des groupes à la page 483).

Illustration 348 : Liste de groupes

Une exception a été ajoutée au Content Control.

Vous pouvez ensuite configurer le Content Control pour le groupe (voir Configurer le Content Control à la page 477), modifier la priorité du groupe (voir Modifier les priorités des groupes à la page 483) ou supprimer le groupe du Content Control (voir Supprimer un groupe de Content Control à la page 485).

Configurer le Content Control

Vous avez activé le Content Control (voir Activer le Content Control à la page 474).

Dans le module **Paramètres de sécurité** > **Content Control**, vous pouvez configurer le Content Control. Vous pouvez modifier les paramètres par défaut du domaine et les paramètres des groupes individuels.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.

4. Sous **Groupes concernés**, sélectionnez si vous souhaitez modifier les paramètres par défaut ou les paramètres d'un groupe.

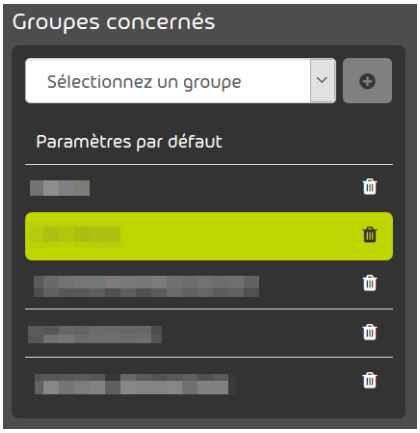


Illustration 349 : Sélectionner les paramètres par défaut ou un groupe

- Pour modifier les paramètres de tous les utilisateurs du domaine qui n'appartiennent pas à l'un des groupes énumérés, sélectionnez **Par défaut**.
- Pour modifier les paramètres d'un groupe, sélectionnez le groupe.

Votre sélection est mise en évidence en vert.

5. Allez à **Paramètres** > **Pour les courriels entrants** pour configurer le Content Control pour les courriels entrants.

6. Sous **Taille de courriel maximale (MB)**, saisissez la taille maximale autorisée pour un courriel en mégabytes.

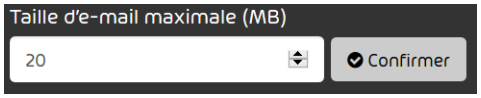


Illustration 350 : Saisir la taille maximale des courriels

REMARQUE :

La taille maximale du courriel ne doit pas dépasser la taille limite de votre serveur de messagerie. La taille maximale du courriel correspond à la charge utile du courriel. La charge utile est composée de la taille du courriel et de ses pièce-jointes sur l'ordinateur du destinataire. La taille réelle du courriel qui inclut des données supplémentaires requises pour la transmission du courriel peut être environ un tiers plus grande. Car la taille limite de votre serveur de messagerie correspond à la taille réelle, la valeur du champ **Taille de courriel maximale (MB)** doit être calculée en fonction de la taille réelle maximale. La valeur indicative est de 67 % de la taille réelle maximale.

Exemple : Si la taille limite du serveur cible est de 10 Mo, une taille maximale du courriel de 6,7 Mo doit être saisie dans le champ.

REMARQUE :

Le champ **Taille de courriel maximale (MB)** accepte des valeurs jusqu'à 150 Mo maximum.

7. Cliquez sur **Confirmer** pour enregistrer les modifications.

8.

REMARQUE :

Vous ne pouvez définir une valeur que pour les courriels entrants. Les courriels sortants avec des pièces-jointes filtrées sont bloqués et l'expéditeur reçoit une notification d'échec de remise.

Sous **Traitement de pièces-jointes filtrées**, sélectionnez la manière de traiter des courriels avec pièces-jointes filtrées.

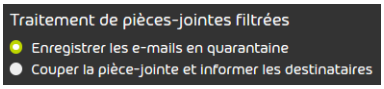


Illustration 351 : Sélectionner le traitement de pièces-jointes filtrées

- Pour mettre les courriels avec des pièces-jointes filtrées en quarantaine et éviter qu'ils ne soient envoyés aux destinataires, sélectionnez **Enregistrer les courriels en quarantaine**.
- Pour séparer les pièces-jointes filtrées des courriels et envoyer à la place les courriels avec des pièces-jointes générées automatiquement, qui indiquent que les pièces-jointes ont été supprimées, sélectionnez **Couper la pièce-jointe et informer les destinataires**.

9. Sélectionnez les pièces-jointes à filtrer. Pour filtrer les pièces-jointes, activez le bouton correspondant.

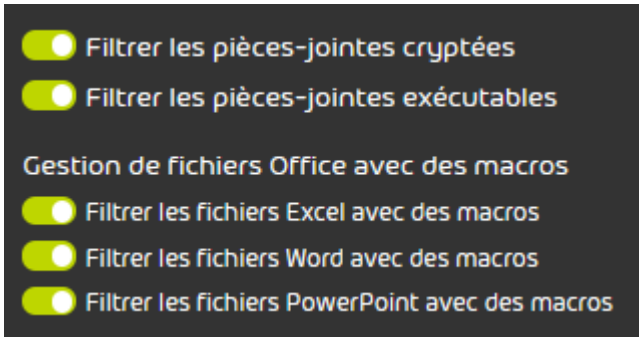


Illustration 352 : Filtrer les pièces-jointes

- Sélectionnez **Filtrer les pièces-jointes cryptées** pour filtrer les pièces-jointes cryptées avec les extensions de fichier suivantes :
  - .dot
  - .doc
  - .docx
  - .xls
  - .xlsx
  - .ppt
  - .pptx
  - .pdf
  - .zip
  - .rar
  - .7z
  - .gz
- Sélectionnez **Filtrer les pièces-jointes exécutables** pour filtrer tous les types de fichiers qui tombent sous le mot-clé .executable (voir Vue d' ensemble des mots-clés collectifs à la page 473).

- Sélectionnez **Filtrer les fichiers Excel avec des macros** pour filtrer tous les types de fichiers qui tombent sous le mot-clé .xslmacro (voir Vue d'ensemble des mots-clés collectifs à la page 473).
- Sélectionnez **Filtrer les fichiers Word avec des macros** pour filtrer tous les types de fichiers qui tombent sous le mot-clé .docmacro (voir Vue d'ensemble des mots-clés collectifs à la page 473).
- Sélectionnez **Filtrer les fichiers PowerPoint avec des macros** pour filtrer tous les types de fichiers qui entrent dans le cadre du terme générique .pptmacro (voir Vue d'ensemble des mots-clés collectifs à la page 473).

10.

REMARQUE :

Vous pouvez utiliser des mots-clés pour filtrer des groupes de types de fichiers (voir Vue d'ensemble des mots-clés collectifs à la page 473).

IMPORTANT :

Le Content Control vérifie non seulement l'extension du fichier mais aussi le type MIME du fichier. Le type MIME peut différer de l'extension de fichier.

Si vous filtrez les fichiers de type gzip, tous les fichiers avec le type MIME application / gzip seront également filtrés.

Illustration 353 : Exemple

Pour filtrer les pièces-jointes avec d'autres extensions de fichier, saisissez l'extension de fichier dans le champ sous **Extensions de fichiers interdites (p. ex., « .jpg »)** et cliquez sur **Ajouter**.

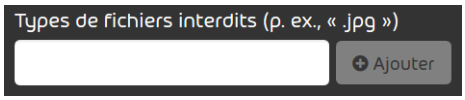


Illustration 354 : Filtrer des types de fichiers

Le type de fichier est indiqué ci-dessous.

11. **IMPORTANT :**

    Le Content Control ouvre et analyse les archives des formats .rar, .zip et .7z. Les archives d'autres formats ne sont pas vérifiées. Si les archives sont imbriquées, le Content Control vérifie les archives jusqu'au 4e niveau. Le Content Control vérifie un maximum de 8 archives par niveau. Le Content Control vérifie un maximum de 1 000 fichiers dans les archives par courriel.

    Pour filtrer les fichiers de certains types de fichiers des archives, procédez comme suit.

    - Pour copier les types de fichiers énumérés ci-dessus, cochez la case **Reprendre les extensions de fichiers interdites de ci-dessus** sous **Extensions de fichiers interdites dans les archives (p. ex., « .png »)**.
    - Pour filtrer les pièces-jointes avec d'autres types de fichiers, saisissez le type de fichier dans le champ sous **Extensions de fichiers interdites dans les archives (p. ex., « .png »)** et cliquez sur **Ajouter**.

12. Allez à **Paramètres** > **Pour les courriels sortants** pour configurer le Content Control pour les courriels sortants.
13. Paramétrez le Content Control pour les courriels sortants.
    - Pour appliquer les paramètres des courriels entrants aux courriels sortants, activez le bouton **Utiliser les paramètres de courriels entrants**.
    - Pour configurer des paramètres différents pour les courriels sortants et pour les courriels entrants, suivez la même procédure que les étapes précédentes pour les courriels entrants.

Le Content Control a été configuré.

Modifier les priorités des groupes

Vous avez ajouté plusieurs groupes au Content Control (voir Ajouter un groupe au Content Control à la page 475).

Dans le module **Paramètres de sécurité** > **Content Control**, les groupes sont classés en fonction de leur priorité. Les priorités des groupes sont affichées sous **Groupes concernés** dans la colonne

Priorité. Plus le nombre est bas, plus un groupe est prioritaire. Si une boîte aux lettres appartient à plusieurs groupes dans le module **Paramètres de sécurité** > **Content Control**, les règles du groupe qui dispose de la priorité la plus élevée seront appliquées à la boîte aux lettres. Vous pouvez modifier les priorités des groupes.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour les groupes duquel vous souhaitez modifier les priorités dans le module **Content Control**.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.
4. Sous **Groupes concernés**, sélectionnez le groupe dont vous souhaitez modifier la priorité.
5. Facultatif : Modifiez la priorité du groupe en déplaçant le groupe dans la liste.
   a) Cliquez sur les six points à côté du groupe et maintenez le bouton gauche de la souris enfoncé.

Illustration 355 : Déplacer un groupe

   b) Faites glisser le groupe vers la position qui correspond à la nouvelle priorité.

   c) Relâchez le bouton gauche de la souris.

➔ Le groupe est placé à la nouvelle position. Les priorités de tous les groupes qui se sont déplacés dans la liste sont actualisées.

6. Écrasez la priorité du groupe.
   a) Double-cliquez sur la priorité à côté du groupe.

➔ Le nombre peut maintenant être modifié.

Illustration 356 : Champ de saisie pour la priorité

b) Saisissez le nombre de la nouvelle priorité dans le champ de saisie ou sélectionnez le nombre à l'aide des flèches de sélection.

c) Confirmez la nouvelle priorité à l'aide de la touche Entrée.

La priorité du groupe est enregistrée. Le groupe est placé à la position qui correspondant à la nouvelle priorité. Les priorités de tous les groupes qui se sont déplacés dans la liste sont actualisées.

Les priorités des groupes ont été modifiées.

Supprimer un groupe de Content Control

Vous avez ajouté un groupe au Content Control (voir Ajouter un groupe au Content Control à la page 475).

Dans le module **Paramètres de sécurité** > **Content Control**, vous pouvez supprimer un groupe de Content Control afin que les paramètres standard de Content Control soient à nouveau appliqué au groupe.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.

4. Cliquez sur le symbole de croix à côté du groupe.

Illustration 357 : Supprimer un groupe

Un message d'avertissement apparaît.

5. Cliquez sur **Confirmer**.

Le groupe est supprimé du Content Control.

Un groupe a été supprimé du Content Control. Les paramètres par défaut du Content Control sont appliqués aux membres du groupe.

Désactiver le Content Control

Vous avez activé le Content Control (voir Activer le Content Control à la page 474).

Dans le module **Paramètres de sécurité** > **Content Control**, vous pouvez désactiver le Content Control pour un domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Content Control**.

4. Actionnez le bouton **Activer Content Control**.

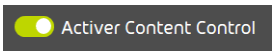


Illustration 358 : Désactiver le Content Control

Un message d'avertissement apparaît.

5. Cliquez sur **Confirmer** pour supprimer irrévocablement tous les paramètres du Content Control du domaine.

Illustration 359 : Confirmer

Le Content Control a été désactivé pour un domaine. Tous les paramètres du Content Control ont été irrévocablement supprimés pour le domaine.

Compliance Filter

À propos du Compliance Filter

Avec le Compliance Filter, les administrateurs côté clients peuvent définir des règles de filtre propres, par ex. pour catégoriser les courriels entrants comme **Valide**, **Spam** ou **Threat**(voir « Catégories de courriels » dans le manuel du Control Panel). En outre, des courriels peuvent être refusés, transférés par un autre serveur ou envoyés à d'autres destinataires. Pour une classification des règles de filtre du Compliance Filter dans l'ordre des règles de tous nos services, voir Ordre des règles dans tous les services à la page 451.

PRUDENCE :

Des règles de filtrage incorrectes affectent le trafic de courriels et peuvent suspendre nos services.

Le Compliance Filter ne convient pas à la réécriture d'adresses.

Le Compliance Filter peut vérifier aussi bien les courriels entrants que sortants. Après l'activation du Compliance Filter (voir Activer le Compliance Filter à la page 491), les administrateurs peuvent définir des règles de filtre côté client pour les types suivants :

- **En-tête**
- **Corps**
- **Avancé**

Des expressions régulières peuvent être utilisées dans les conditions des règles de filtre (voir Expressions régulières à la page 539). Les administrateurs côté clients définissent une action pour chaque règle de filtre. Cette action est appliquée automatiquement aux courriels concernés par la règle de filtre. Pour de plus amples informations sur les règles de filtre, voir Règles de filtre à la page 492. Au total, jusqu'à 1500 règles de filtre peuvent être définies par client.

Outre les règles de filtre pour des expressions individuelles, il est possible de créer des règles de filtre plus complexes et plus précises à l'aide de dictionnaires pouvant contenir chacun jusqu'à 15 000 expressions littérales ou jusqu'à 1 000 expressions régulières (voir Dictionnaires à la page 531). Les administrateurs côté clients peuvent créer et gérer jusqu'à 250 dictionnaires pour leur domaine principal. En particulier, les dictionnaires contenant des expressions régulières réduisent considérablement le temps nécessaire à la création et à la gestion des règles de filtre.

Pour pouvoir activer et paramétrer le Compliance Filter pour un domaine, la Spam and Malware Protection (voir « Spam and Malware Protection » dans le manuel du Control Panel) doit être activée pour le domaine. Dès que la Spam and Malware Protection est désactivée, le Compliance Filter est également désactivé et ne peut plus être paramétré.

Les administrateurs côté clients peuvent désactiver le Compliance Filter s'ils ne souhaitent plus l'utiliser (voir Désactiver le Compliance Filter à la page 553).

Ordre des règles dans tous les services

Les règles de la Spam and Malware Protection (voir « Spam and Malware Protection » dans le manuel du Control Panel) ont une certaine priorité dans laquelle elles sont traitées. Dès qu'une règle avec une priorité supérieure intervient, les règles avec une priorité inférieure ne sont plus traitées. Cela peut entraîner le blocage du courriel malgré l'entrée dans la liste des expéditeurs autorisés de l'adresse de l'expéditeur car l'adresse IPv4 du serveur expéditeur a été entrée sur la liste RBL des expéditeurs interdits.

Ordre des règles (priorité décroissante de haut en bas) :

Courriels entrants

1. Liste RBL (bloquer)
2. Détection de spams de masse (bloquer)
3. Compliance Filter
4. Email Authentication (bloquer)
5. Vérification de la présence de contenus malveillants (mettre en quarantaine)
6. Email Authentication (mettre en quarantaine)
7. Content Control, si activé (mettre en quarantaine)
8. Autorisation basée sur l'utilisateur (distribuer)
9. Interdiction basée sur l'utilisateur (mettre en quarantaine)

10. Autorisation administrative (distribuer)

> **REMARQUE :**
>
> La création administrative d'expéditeurs autorisés est un cas particulier parmi les règles. En effet, les administrateurs peuvent choisir, pour les entrées d'expéditeurs autorisés au niveau d'un domaine, quels filtres seront contournés par l'entrée (voir « Créer une entrée d'expéditeur interdit pour un domaine » dans le manuel du Control Panel). Les courriels concernés sautent donc les filtres sélectionnés lorsqu'ils sont traités. Cela vaut également pour les filtres qui se trouvent dans la liste avant les expéditeurs autorisés administratifs. La position à laquelle les expéditeurs autorisés administratifs sont classés dans la liste fait référence au réglage par défaut des entrées des expéditeurs autorisés au niveau d'un domaine. Par défaut, les entrées contournent le filtrage du spam comme un seul filtre.

11. Interdiction administrative (mettre en quarantaine)
12. Autorisation générale (distribuer)
13. Règles générales de spam (mettre en quarantaine)
14. Filtre infomail (mettre en quarantaine)

> **REMARQUE :**
>
> Le Compliance Filter (voir À propos du Compliance Filter à la page 487) est appliqué avant le Content Control (voir À propos du Content Control à la page 472). Par conséquent, les administrateurs peuvent créer des exceptions au Content Control avec des règles du Compliance Filter qui classent les courriels dans la catégorie **Valide**.
>
> Pour le Content Control en revanche, il n'est pas possible de créer des exceptions via les expéditeurs autorisés et les expéditeurs interdits définis par l'utilisateur, ni via les expéditeurs interdits administratifs, car ces règles ne sont appliquées qu'après le Content Control. Seule la création administrative d'expéditeurs autorisés permet de contourner le Content Control.

Courriels sortants

1. Liste RBL
2. Compliance Filter
3. Vérification de la présence de contenus malveillants
4. Content Control, si activé

Activer le Compliance Filter

Vous avez activé la Spam and Malware Protection (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel) pour le domaine pour lequel vous souhaitez activer le Compliance Filter.

Le module **Paramètres de sécurité** > **Compliance Filter** vous permet d'activer le Compliance Filter afin de pouvoir créer certaines règles pour le filtrage de courriels (voir Règles de filtre à la page 492).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer le Compliance Filter.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Activez le bouton **Activer Compliance Filter**.

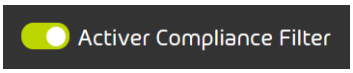


Illustration 360 : Activer le Compliance Filter

Le Compliance Filter est activé.

Le Compliance Filter a été activé. Le Compliance Filter peut être utilisé dès que les règles de filtre ont été créées.

Vous pouvez ensuite créer des règles de filtre (voir Règles de filtre à la page 492) et des dictionnaires (voir Dictionnaires à la page 531) pour le Compliance Filter.

Règles de filtre

Le Compliance Filter vérifie les courriels d'un domaine. Dans le module **Compliance Filter**, les administrateurs côté clients peuvent gérer les règles de filtre pour les courriels entrants et sortants. Les administrateurs peuvent créer des règles de filtre pour les courriels entrants (voir Créer une règle de filtre pour les courriels entrants à la page 493) et sortants (voir Créer une règle de filtre pour les courriels sortants à la page 499). Les règles de filtre créées sont affichées dans deux tableaux (voir Affichage des règles de filtre à la page 506).

REMARQUE :

Il est possible de créer jusqu'à 1500 règles de filtre pour un domaine principal.

Les administrateurs côté clients peuvent définir une action (voir Actions pour les règles de filtre à la page 508) pour chaque règle de filtre. L'action est exécutée dès que la règle de filtre est appliquée à un courriel.

Les administrateurs côté clients choisissent en outre un type pour chaque règle de filtre (voir Types de règles de filtre à la page 511). Le type de règle de filtre permet de définir à quels courriels s'applique la règle de filtre.

Une condition possible pour les règles de filtre sont les destinataires auxquels un courriel est envoyé. Si un courriel est envoyé à plusieurs destinataires et qu'une règle de filtre s'applique à certains d'entre eux, l'action ne s'appliquera qu'à l'envoi du courriel aux destinataires auxquels la règle de filtre s'applique. Différentes actions sont ainsi possibles pour différents destinataires du même courriel.

Les administrateurs côté clients peuvent modifier les règles de filtre existantes par la suite (voir Éditer la règle de filtre à la page 517). En outre, les administrateurs peuvent modifier la priorité des règles de filtre (voir Modifier la priorité d' une règle de filtre à la page 519). La priorité permet d'élaborer l'ordre des règles de filtre du Compliance Filter. D'autres informations concernant l'ordre des règles de filtre du Compliance Filter sont disponibles sous Ordre des règles de filtre à la page 521.

Si une règle de filtre ne doit pas être utilisée temporairement, les administrateurs côté clients peuvent la désactiver (voir Désactiver une règle de filtre du Compliance Filter à la page 528). Les règles de filtre désactivées peuvent être activées à nouveau ultérieurement (voir Activer une règle de filtre à la page 527).

Dès qu'une règle de filtre n'est plus nécessaire, les administrateurs côté clients peuvent la supprimer (voir Supprimer une règle de filtre du Compliance Filter à la page 529).

Créer une règle de filtre pour les courriels entrants

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez créer les règles de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487) pour les courriels entrants.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer la règle de filtre.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.
5. Dans **Règles pour des e-mails entrants**, cliquez sur **Ajouter règle**.

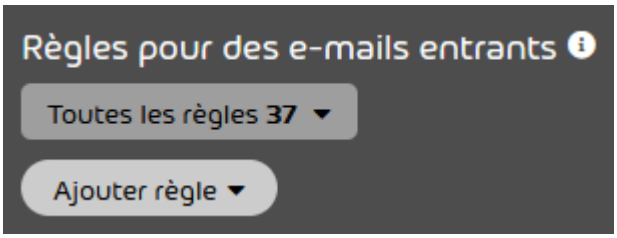


Illustration 361 : Ajouter une règle

6. Sous **Action**, sélectionnez la conduite à tenir avec les courriels auxquels s'appliquent les règles de filtre. Vous pouvez choisir parmi les actions suivantes :

   - **Rejeter**
   - **Changer le destinataire**
   - **Rediriger**
   - **Ajouter CCI**
   - **Marquer comme « Valide »**
   - **Marquer comme « Spam »**
   - **Marquer comme « Threat »**

   REMARQUE :

   Vous trouverez une explication des actions sous Actions pour les règles de filtre à la page 508.

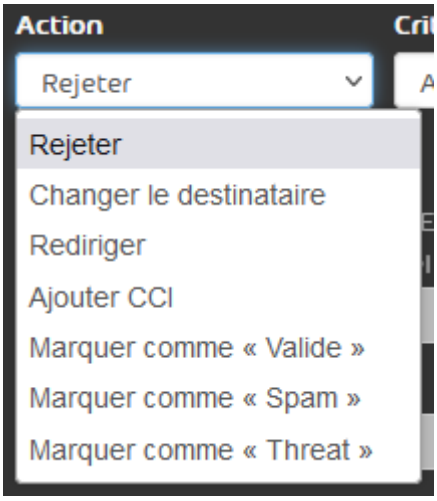


Illustration 362 : Sélectionner une action

- Si des informations supplémentaires sont nécessaires pour l'action sélectionnée, un champ supplémentaire apparaît sous le menu déroulant. Pour plus d'informations concernant les champs supplémentaires, voir Actions pour les règles de filtre à la page 508.

7. Dans **Conditions**, sélectionnez le type de règle de filtre. Vous avez les options suivantes :

   - **En-tête** : la règle de filtre s'applique à tous les courriels dont l'entête contient un terme de recherche précis.
   - **Corps** : la règle de filtre s'applique à tous les courriels dont le corps contient un terme de recherche précis.
   - **Avancé** : Vous pouvez spécifier l'expéditeur, le destinataire, l'adresse IPv4 et le nom d'hôte des courriels. Vous pouvez également définir des mots-clés pour l'objet et la pièce jointe des courriels et une taille maximale du courriel. La règle de filtre s'applique à tous les courriels présentant les caractéristiques spécifiées.

   REMARQUE :

   Le type de règle de filtre permet de définir à quels courriels doit s'appliquer la règle de filtre.

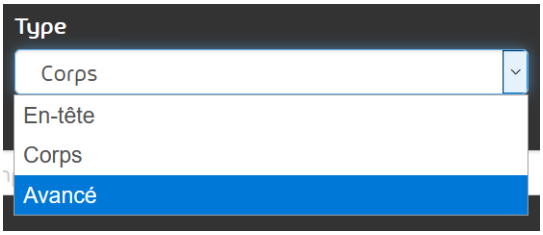


Illustration 363 : Sélectionner le type de règle de filtre

Les champs pour la configuration des règles de filtre s'affichent dans le menu déroulant. La nature des champs qui s'affichent dépend du type de règle de filtre sélectionné.

REMARQUE :

Sous Types de règles de filtre à la page 511 se trouvent un aperçu et des explications des champs disponibles pour chaque type de règle de filtre.

8. Si vous avez sélectionné le type **Avancé**, suivez les étapes suivantes :

   a) Sous **Conditions**, sélectionnez le lien logique entre les conditions qui doit s'appliquer à la règle de filtre. Vous avez les options suivantes :

      - **Correspond à toutes les conditions** : Toutes les conditions sélectionnées doivent être remplies pour que la règle de filtre soit appliquée à un courriel. Ce lien correspond à une logique ET.
      - **Correspond à n'importe quelle condition** : Il suffit qu'une des conditions sélectionnées soit remplie pour que la règle de filtre soit appliquée à un courriel. Ce lien correspond à une logique OU.

   b) Cochez les cases des conditions qui doivent s'appliquer à la règle de filtre.

Les champs de saisie des conditions sélectionnées sont débloqués.

   c) Si le champ de saisie de la condition sélectionnée contient un menu déroulant, sélectionnez le type de saisie que vous souhaitez effectuer. Vous avez les options suivantes :

      - **Expression littérale / régulière** : La valeur saisie est interprétée comme une expression littérale ou régulière.
      - **Figure dans le dictionnaire** : La valeur saisie est interprétée comme le nom d'un dictionnaire (voir Dictionnaires à la page 531) qui est référencé dans la condition. La condition est remplie si la valeur correspondante du courriel correspond à une entrée du dictionnaire référencé.
      - **Ne figure pas dans le dictionnaire** : La valeur saisie est interprétée comme le nom d'un dictionnaire (voir Dictionnaires à la page 531) qui est référencé dans la condition. La

condition est remplie si la valeur correspondante du courriel ne correspond à aucune entrée du dictionnaire référencé.

d) Si vous avez sélectionné la condition **Expéditeur** ou **Destinataire**, choisissez à quel champ du courriel la valeur saisie doit se référer. Vous avez les options suivantes :

- **En raison de l'enveloppe** : La valeur saisie doit correspondre à l'adresse qui a été transmise comme paramètre de **MAIL FROM:** (adresse de l'expéditeur) ou **RCPT TO:** (adresse du destinataire) lors de l'envoi du courriel.
- **En raison de l'en-tête** : La valeur saisie doit correspondre à l'adresse qui est indiquée dans le champ **From** (adresse de l'expéditeur) ou **To** dans l'entête du courriel.
- **En raison de tous les deux** : L'adresse d'expéditeur saisie doit être indiquée soit comme paramètre de **MAIL FROM:**, soit dans le champ **From** de l'entête du courriel. L'adresse de destinataire saisie doit être indiquée soit comme paramètre de **RCPT TO:**, soit dans le champ **To** de l'entête du courriel.

9. Selon le type de saisie, saisissez un terme de recherche, une valeur ou le nom d'un dictionnaire dans les champs de saisie des conditions.

> **REMARQUE :**
>
> Un terme de recherche est également trouvé sous forme d'expression littérale ou régulière s'il est entouré de texte.

> **REMARQUE :**
>
> Pour définir des règles plus précises et polyvalentes, vous pouvez utiliser des expressions régulières. Vous trouverez une description de la structure et de la fonctionnalité d'expressions régulières sous Expressions régulières à la page 539 et Explication des expressions régulières à la page 541. Sous Exceptions pour les expressions régulières à la page 549, vous trouverez une vue d'ensemble des caractères qui ne sont pas pris en charge.
>
> Des expressions régulières ne peuvent être utilisées que dans les règles du type **Avancé**.

> **REMARQUE :**
>
> Dans le champ **Plus grand que**, saisissez la taille maximale pour un courriel en mégabytes.

10. Facultatif : Saisissez une description de la règle de filtre sous **Description (optionnelle)**.

Illustration 364 : Décrire la règle de filtre

11. Cliquez sur **Ajouter**.

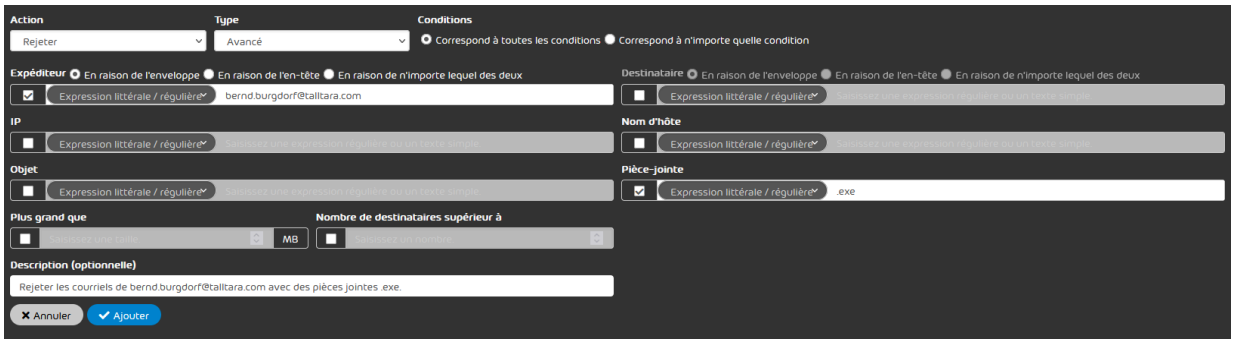


Illustration 365 : Ajouter une règle de filtre

La règle de filtre est ajoutée au tableau sous **Règles pour des e-mails entrants** (voir Affichage des règles de filtre à la page 506). La règle de filtre se voit accorder la priorité la plus basse parmi toutes les règles de filtre existantes et est placée à la fin du tableau. La règle de filtre est activée.

Une règle de filtre a été créée pour les courriels entrants.

Vous pouvez ensuite modifier la règle de filtre (voir Éditer la règle de filtre à la page 517), changer la priorité de la règle de filtre (voir Modifier la priorité d' une règle de filtre à la page 519), désactiver la règle de filtre temporairement (voir Désactiver une règle de filtre du Compliance Filter à la page 528) ou la supprimer (voir Supprimer une règle de filtre du Compliance Filter à la page 529).

Créer une règle de filtre pour les courriels sortants

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez créer les règles de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487) pour les courriels sortants.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer la règle de filtre.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.
5. Dans **Règles pour des e-mails sortants**, cliquez sur **Ajouter règle**.

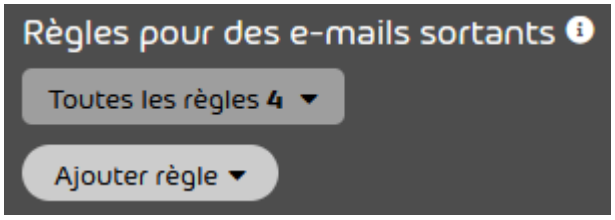


Illustration 366 : Ajouter une règle

6. Sous **Action**, sélectionnez la conduite à tenir avec les courriels auxquels s'appliquent les règles de filtre. Vous pouvez choisir parmi les actions suivantes :

   - **Rejeter**
   - **Changer le destinataire**
   - **Rediriger**
   - **Ajouter CCI**
   - **Notifier l' expéditeur**

   REMARQUE :

   Vous trouverez une explication des actions sous Actions pour les règles de filtre à la page 508.

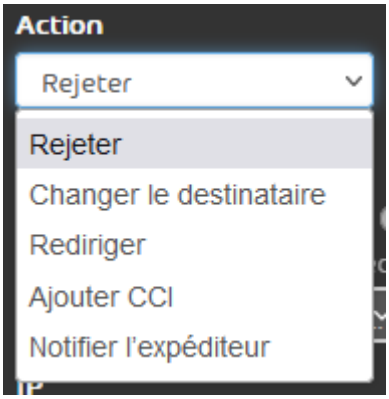


Illustration 367 : Sélectionner une action

Si des informations supplémentaires sont nécessaires pour l'action sélectionnée, un champ supplémentaire apparaît sous le menu déroulant. Pour plus d'informations concernant les champs supplémentaires, voir Actions pour les règles de filtre à la page 508.

7. Dans **Type**, sélectionnez le type de règle de filtre. Cela permet de déterminer les courriels auxquels la règle de filtre doit être appliquée. Vous avez les options suivantes :

   - **En-tête** : la règle de filtre s'applique à tous les courriels dont l'entête contient un terme de recherche précis.
   - **Corps** : la règle de filtre s'applique à tous les courriels dont le corps contient un terme de recherche précis.
   - **Avancé** : Vous pouvez spécifier l'expéditeur, le destinataire, l'adresse IPv4 et le nom d'hôte des courriels. Vous pouvez également définir des mots-clés pour l'objet et la pièce jointe des courriels et une taille maximale du courriel. La règle de filtre s'applique à tous les courriels présentant les caractéristiques spécifiées.

   REMARQUE :

   Le type de règle de filtre permet de définir à quels courriels doit s'appliquer la règle de filtre.

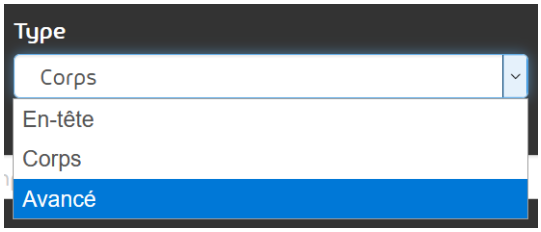


Illustration 368 : Sélectionner le type de règle de filtre

Les champs pour la configuration des règles de filtre s'affichent dans le menu déroulant. La nature des champs qui s'affichent dépend du type de règle de filtre sélectionné.

REMARQUE :

Sous Types de règles de filtre à la page 511 se trouvent un aperçu et des explications des champs disponibles pour chaque type de règle de filtre.

8. Si vous avez sélectionné le type **Avancé**, suivez les étapes suivantes :

   a) Sous **Conditions**, sélectionnez le lien logique entre les conditions qui doit s'appliquer à la règle de filtre. Vous avez les options suivantes :

      - **Correspond à toutes les conditions** : Toutes les conditions sélectionnées doivent être remplies pour que la règle de filtre soit appliquée à un courriel. Ce lien correspond à une logique ET.
      - **Correspond à n'importe quelle condition** : Il suffit qu'une des conditions sélectionnées soit remplie pour que la règle de filtre soit appliquée à un courriel. Ce lien correspond à une logique OU.

   b) Cochez les cases des conditions qui doivent s'appliquer à la règle de filtre.

Les champs de saisie des conditions sélectionnées sont débloqués.

   c) Si le champ de saisie de la condition sélectionnée contient un menu déroulant, sélectionnez le type de saisie que vous souhaitez effectuer. Vous avez les options suivantes :

      - **Expression littérale / régulière** : La valeur saisie est interprétée comme une expression littérale ou régulière.
      - **Figure dans le dictionnaire** : La valeur saisie est interprétée comme le nom d'un dictionnaire (voir Dictionnaires à la page 531) qui est référencé dans la condition. La condition est remplie si la valeur correspondante du courriel correspond à une entrée du dictionnaire référencé.
      - **Ne figure pas dans le dictionnaire** : La valeur saisie est interprétée comme le nom d'un dictionnaire (voir Dictionnaires à la page 531) qui est référencé dans la condition. La

condition est remplie si la valeur correspondante du courriel ne correspond à aucune entrée du dictionnaire référencé.

d) Si vous avez sélectionné la condition **Expéditeur** ou **Destinataire**, choisissez à quel champ du courriel la valeur saisie doit se référer. Vous avez les options suivantes :

- **En raison de l'enveloppe** : La valeur saisie doit correspondre à l'adresse qui a été transmise comme paramètre de **MAIL FROM:** (adresse de l'expéditeur) ou **RCPT TO:** (adresse du destinataire) lors de l'envoi du courriel.
- **En raison de l'en-tête** : La valeur saisie doit correspondre à l'adresse qui est indiquée dans le champ **From** (adresse de l'expéditeur) ou **To** dans l'entête du courriel.
- **En raison de tous les deux** : L'adresse d'expéditeur saisie doit être indiquée soit comme paramètre de **MAIL FROM:**, soit dans le champ **From** de l'entête du courriel. L'adresse de destinataire saisie doit être indiquée soit comme paramètre de **RCPT TO:**, soit dans le champ **To** de l'entête du courriel.

9. Selon le type de saisie, saisissez un terme de recherche, une valeur ou le nom d'un dictionnaire dans les champs de saisie des conditions.

> **REMARQUE :**
>
> Un terme de recherche est également trouvé sous forme d'expression littérale ou régulière s'il est entouré de texte.

> **REMARQUE :**
>
> Pour définir des règles plus précises et polyvalentes, vous pouvez utiliser des expressions régulières. Vous trouverez une description de la structure et de la fonctionnalité d'expressions régulières sous Expressions régulières à la page 539 et Explication des expressions régulières à la page 541. Sous Exceptions pour les expressions régulières à la page 549, vous trouverez une vue d'ensemble des caractères qui ne sont pas pris en charge.
>
> Des expressions régulières ne peuvent être utilisées que dans les règles du type **Avancé**.

> **REMARQUE :**
>
> Dans le champ **Plus grand que**, saisissez la taille maximale pour un courriel en mégabytes.

10. Facultatif : Saisissez une description de la règle de filtre sous **Description (optionnelle)**.

Illustration 369 : Décrire la règle de filtre

11. Cliquez sur **Ajouter**.

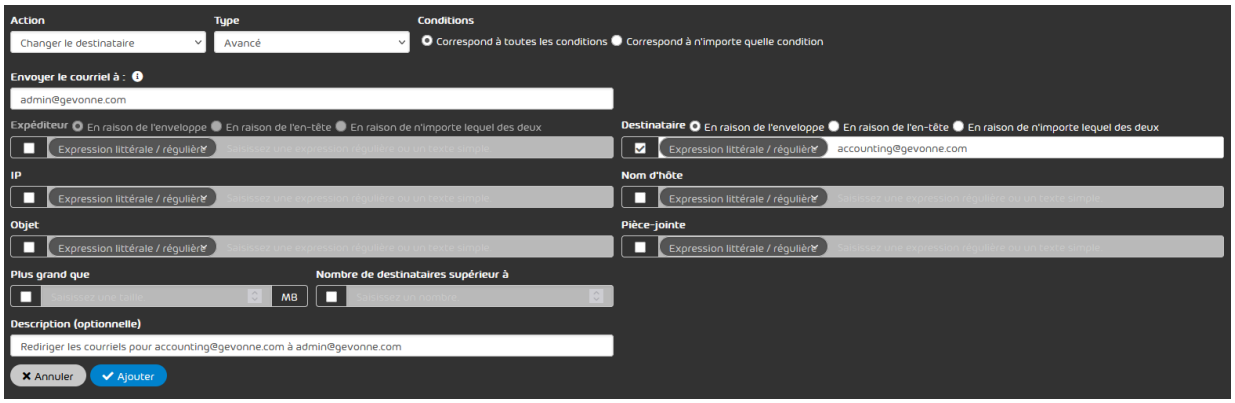


Illustration 370 : Ajouter une règle de filtre

La règle de filtre est ajoutée au tableau sous **Règles pour des e-mails sortants** (voir Affichage des règles de filtre à la page 506). La règle de filtre se voit accorder la priorité la plus basse parmi toutes les règles de filtre existantes et est placée à la fin du tableau. La règle de filtre est activée.

Une règle de filtre a été créée pour les courriels sortants.

Vous pouvez ensuite modifier la règle de filtre (voir Éditer la règle de filtre à la page 517), changer la priorité de la règle de filtre (voir Modifier la priorité d'une règle de filtre à la page 519), désactiver la règle de filtre temporairement (voir Désactiver une règle de filtre du Compliance Filter à la page 528) ou la supprimer (voir Supprimer une règle de filtre du Compliance Filter à la page 529).

Affichage des règles de filtre

Les règles de filtre des courriels entrants et sortants sont affichées après leur création dans le tableau correspondant sous les sections **Règles pour des e-mails entrants** et **Règles pour des e-mails sortants**.

Les deux tableaux contiennent les colonnes suivantes :

- **Priorité** : Priorité d'application des règles de filtre. Une règle de filtre avec un nombre plus petit dans ce champ intervient plus rapidement qu'une règle de filtre avec un nombre plus grand. Les règles de filtre sont classées par ordre de priorité décroissante dans le tableau.
- **Actif** : Le fait de cocher la case indique que la règle de filtre est activée.
- **Action** : On indique ici l'action qui sera exécutée par la règle de filtre.
  - Actions pour courriels entrants : **Changer le destinataire**, **Rediriger**, **Ajouter CCI**, **Marquer comme « Valide »**, **Marquer comme « Spam »**, **Marquer comme « Threat »**.
  - Actions pour les courriels sortants : **Rejeter**, **Changer le destinataire**, **Rediriger**, **Ajouter CCI**, **Notifier l'expéditeur**.

  REMARQUE :

  Les actions disponibles sont décrites au chapitre Actions pour les règles de filtre à la page 508.
- **Type** : Le type de règle de filtre est indiqué ici.
- **Conditions** : Les conditions de filtre sont indiquées ici dans la langue du système paramétrée. Si un dictionnaire est référencé dans une règle avancée, il est indiqué par la lettre **D**. Dans l'exemple suivant, les expéditeurs du dictionnaire **forbiddensenders** sont pris en compte pour la règle : **Expéditeur : ?A=?D=forbiddensenders**. Les entrées d'un dictionnaire peuvent également être

niées. Dans l'exemple suivant, les expéditeurs du dictionnaire **forbiddensenders** ne sont pas pris en compte : **Expéditeur : ?A=?D!=forbiddensenders**.

> **REMARQUE :**
>
> Les conditions de filtre **Expéditeur** et **Destinataire** indiquent également le ou les champs auxquels se réfère la valeur saisie (**En raison de l'enveloppe**, **En raison de l'en-tête** et **En raison de tous les deux** tel que décrit dans le chapitre Types de règles de filtre à la page 511). Cela est indiqué à chaque fois par les lettres **E** (pour **Envelope**), **H** (pour **Header**) et **A** (pour **Any**), indépendamment de la langue.
>
> Par exemple, l'indication **Expéditeur :?E=sophie@michelle.com** signifierait qu'une règle de filtre doit être appliquée aux courriels dont l'expéditeur d'enveloppe est **E=sophie@michelle.com**.

- **Description** : Description attribuée par le créateur de la règle de filtre.
- **ID** : Nombre attribué automatiquement par le système pour identifier la règle de filtre.

Actions pour les règles de filtre

Une action est attribuée à chaque règle de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487). Dès que la règle de filtre est appliquée à un courriel, l'action est exécutée.

Différentes actions sont disponibles pour les courriels entrants et sortants.

Les actions suivantes sont disponibles uniquement pour les courriels entrants :

- **Marquer comme « Valide »**
- **Marquer comme « Spam »**
- **Marquer comme « Threat »**

L'action **Notifier l'expéditeur** est disponible uniquement pour les courriels sortants.

Le tableau suivant décrit toutes les actions pour les règles de filtre dans le module **Compliance Filter**. Si une action est sélectionnée dans le module **Compliance Filter** pour laquelle des indications

complémentaires sont nécessaires, un champ supplémentaire apparaît pour l'action. Ces champs sont également décrits dans le tableau.

Tableau 27 : Actions pour les règles de filtre

ACTION	DESCRIPTION
Rejeter	**ATTENTION :** Le courriel est refusé. Le serveur de messagerie d'envoi est informé de la fin de la connexion par code d'erreur et texte (**554 5.6.9 customer rule based reject by Compliance-Filter**). Pour de plus amples informations, voir « Raisons de catégorisation » dans le manuel du Control Panel. Les informations de l'expéditeur sont sous la responsabilité du serveur de messagerie d'envoi.
Changer le destinataire	Le courriel est envoyé à une ou plusieurs autres adresses courriel au lieu du destinataire initial. Si cette action est sélectionnée, le champ **Envoyer le courriel à :** apparaît. Dans ce champ, les administrateurs côté clients doivent saisir toutes les adresses courriel auxquelles le courriel doit être transféré. Les administrateurs peuvent entrer n'importe quel nombre d'adresses courriel dans le champ. Si plusieurs adresses courriel sont saisies, celles-ci doivent être séparées par un point-virgule.

ACTION	DESCRIPTION
Rediriger	Le courriel est envoyé via une adresse IPv4 ou un autre nom d'hôte. Si cette action est sélectionnée, le champ **IP ou nom d'hôte** apparaît. Dans ce champ, les administrateurs côté clients doivent saisir l'adresse IPv4 ou le nom d'hôte par lequel le courriel doit être redirigé. Les administrateurs ne peuvent saisir qu'une seule adresse IPv4 ou un nom d'hôte.
Ajouter CCI	Un ou plusieurs destinataires BCC sont ajoutés automatiquement au courriel. Si cette action est sélectionnée, le champ **Envoyer le courriel à :** apparaît. Dans ce champ, les administrateurs côté clients doivent saisir les adresses courriel auxquelles des copies cachées du courriel doivent être transférées. Les administrateurs peuvent entrer n'importe quel nombre d'adresses courriel dans le champ. Si plusieurs adresses courriel sont saisies, celles-ci doivent être séparées par un point-virgule.
Notifier l' expéditeur	L'expéditeur est notifié par courriel dès que le courriel sortant est accepté par le serveur de destination.
Marquer comme « Valide »	Le courriel entrant est classé comme **Valide**.
Marquer comme « Spam »	Le courriel entrant est classé comme **Spam**.

ACTION	DESCRIPTION
Marquer comme « Threat »	Le courriel entrant est classé comme **Threat**.

Types de règles de filtre

Lors de la création de règles de filtre dans le module **Compliance Filter** (voir À propos du Compliance Filter à la page 487), les administrateurs côté clients doivent choisir le type de règle de filtre. Avec le type de règle de filtre, les administrateurs définissent les caractéristiques des courriels auxquels la règle de filtre doit être appliquée. Pour chaque type de règle de filtre, le module **Compliance Filter** affiche des champs pour différentes caractéristiques.

Les tableaux suivants présentent un aperçu des champs disponibles pour chaque type de règle de filtre. Les tableaux contiennent des descriptions des caractéristiques et exemples pour les éventuelles saisies.

REMARQUE :

Pour définir des règles plus précises et polyvalentes, des expressions régulières peuvent être utilisées. Pour une description de la structure et de la fonctionnalité d'expressions régulières, voir Expressions régulières à la page 539 et Explication des expressions régulières à la page 541. Pour une vue d'ensemble des caractères qui ne sont pas pris en charge, voir Exceptions pour les expressions régulières à la page 549.

REMARQUE :

Pour simplifier la gestion des conditions, les administrateurs côté clients peuvent regrouper plusieurs expressions dans des dictionnaires. Les dictionnaires peuvent être référencés dans les champs de saisie des conditions des règles de filtre. Pour de plus amples informations sur le fonctionnement, la création et la gestion des dictionnaires, voir Dictionnaires à la page 531.

Tableau 28 : Type En-tête

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Filtre: en-tête	L'entête du courriel est parcouru à la recherche du mot-clé saisi.	Facture

Tableau 29 : Type Corps

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Filtre: corps	Le corps décodé du courriel est parcouru à la recherche du mot-clé saisi. **REMARQUE :** Les pièces jointes sont exclues de la recherche dans le corps du courriel.	Instruction de paiement

Tableau 30 : Type Avancé

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Expéditeur	L'adresse de l'expéditeur du courriel est recherchée selon le terme de recherche saisi ou selon les entrées du dictionnaire référencé (voir Dictionnaires à la page 531). **REMARQUE :** Les administrateurs côté clients peuvent choisir le type d'adresse d'expéditeur à rechercher parmi les options suivantes (voir Créer une règle de filtre pour les courriels entrants) : • **En raison de l'enveloppe** : Adresse d'expéditeur à partir de l'enveloppe (**MAIL FROM:**) • **En raison de l'en-tête** : Adresse d'expéditeur à partir de l'entête (**To:**) • **En raison de tous les deux** : une des deux adresses d'expéditeur au choix	**user@gevonne.com**

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Destinataire	Les adresses de destinataires sont recherchées selon le terme de recherche saisi ou selon les entrées du dictionnaire référencé. **REMARQUE :** Les administrateurs côté clients peuvent sélectionner le type d'adresse de destinataire à rechercher parmi les options suivantes (voir Créer une règle de filtre pour les courriels entrants) : • **En raison de l'enveloppe** : Adresse de destinataire à partir de l'enveloppe (**RCPT TO:**) • **En raison de l'en-tête** : Adresse de destinataire à partir de l'entête (**From:**) • **En raison de tous les deux** : une des deux adresses de destinataire au choix **REMARQUE :**	**user.extern@yahoo.com**

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
IP	L'adresse IPv4 publique du serveur de messagerie expéditeur est recherchée en fonction du terme de recherche saisi ou des entrées du dictionnaire référencé. **REMARQUE :** Saisissez comme critère de recherche l'adresse IPv4 sans masque de sous-réseau.	Correct : **0.0.0.0** Faux : **0.0.0.0/24**
Nom d'hôte	Le nom d'hôte (entrée PTR) obtenu par résolution inverse de l'adresse IPv4 du serveur de messagerie est recherché à partir du terme de recherche saisi ou des entrées du dictionnaire référencé. Selon que la règle s'applique aux courriels entrants ou sortants, il s'agit du nom d'hôte du serveur sortant ou de destination.	**mailserver.domain.com**
Objet	L'objet du courriel est recherché en fonction du terme de recherche saisi ou en fonction des entrées du dictionnaire référencé.	**Spam**

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Pièce-jointe	Les noms de fichiers et les extensions de fichiers des pièces jointes de courriel sont recherchés en fonction du terme de recherche saisi ou en fonction des entrées du dictionnaire référencé. **REMARQUE :** Il est possible d'effectuer une recherche en fonction de l'extension de fichier ou d'une partie du nom du fichier. Pour faire une recherche par extension de fichier, l'extension du fichier doit être saisie comme mot-clé. Pour faire une recherche par une partie du nom du fichier, la partie recherchée doit être saisie comme mot-clé. **REMARQUE :** Pour le Compliance Filter, des mots-clés collectifs ne peuvent pas être appliqués aux pièces-jointes.	**.jpg** **express**

CHAMP	DESCRIPTION	EXEMPLE DE SAISIE
Plus grand que	Le système vérifie si le courriel dépasse la taille saisie. **REMARQUE :** La taille maximale pour un courriel est saisie en mégabytes.	**500**
Nombre de destinataires supérieur à	Le système vérifie si le nombre de destinataires dépasse la taille saisie.	**10**

Éditer la règle de filtre

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491) et créé des règles de filtre pour le Compliance Filter (voir Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez éditer les règles de filtre existantes du Compliance Filter (voir À propos du Compliance Filter à la page 487).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.

5. Dans la liste des règles de filtre pour les courriels entrants ou sortants, cliquez sur la flèche du menu à côté de la règle de filtre que vous souhaitez modifier.

Illustration 371 : Ouvrir le menu

6. Cliquez sur **Éditer règle**.

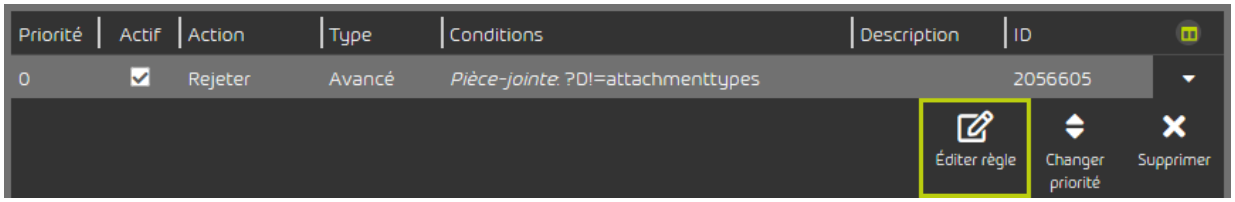


Illustration 372 : Éditer la règle de filtre

Un menu avec les paramètres actuels de la règle de filtre s'ouvre.

7. Modifiez les paramètres en fonction de vos besoins.

> **REMARQUE :**
>
> Vous trouverez de plus amples informations sur Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499.

8. Cliquez sur **Appliquer les modifications**.

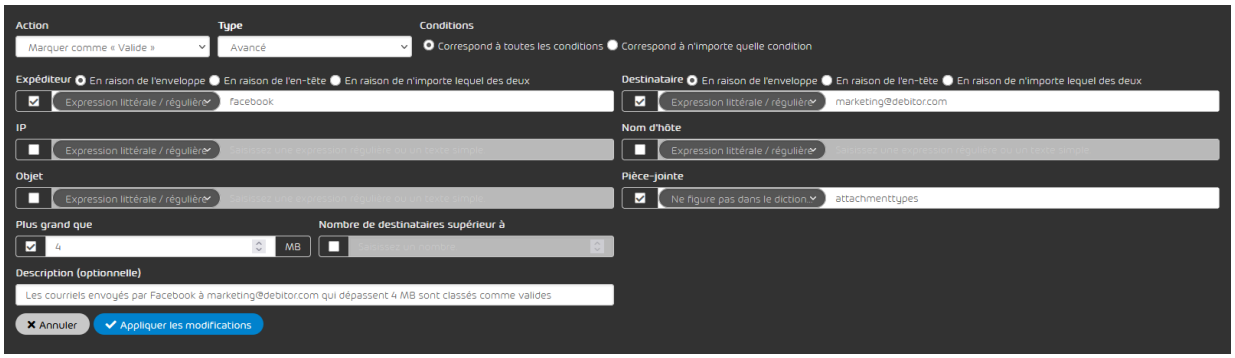


Illustration 373 : Appliquer les modifications

Les modifications sont acceptées.

Une règle de filtre a été éditée.

Modifier la priorité d’ une règle de filtre

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491) et créé des règles de filtre pour le Compliance Filter (voir Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez modifier l'ordre dans lequel les règles de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487) sont traitées. Pour modifier l'ordre des règles de filtre, changez la priorité des règles de filtre.

IMPORTANT :

L'ordre dans lequel les règles de filtre du Compliance Filter sont élaborées dépend non seulement de la priorité, mais également du type des règles de filtre (voir Ordre des règles de filtre à la page 521).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.
5. Dans la liste des règles de filtre pour les courriels entrants ou sortants, cliquez sur la flèche du menu à côté de la règle de filtre dont vous souhaitez modifier la priorité.

Illustration 374 : Ouvrir le menu

Un menu s'ouvre.

6. Cliquez sur **Changer priorité**.

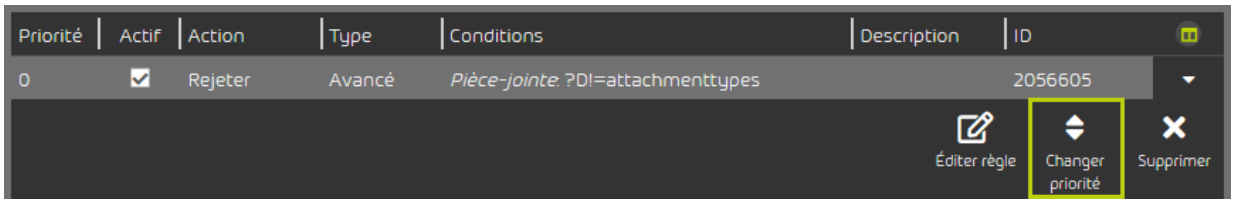


Illustration 375 : Modifier la priorité

Un menu s'ouvre.

7. Saisissez la nouvelle priorité de la règle de filtre sous **Priorité**.

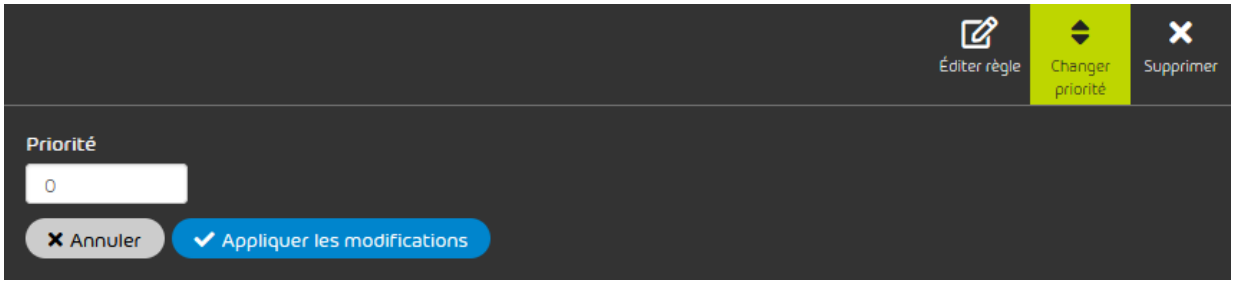


Illustration 376 : Saisir la priorité

8. Cliquez sur **Appliquer les modifications**.

La nouvelle priorité est attribuée à la règle de filtre. La règle de filtre est déplacée à la position dans la liste qui correspond à la nouvelle priorité.

La priorité d'une règle de filtre a été modifiée. Cela a modifié l'ordre dans lequel les règles de filtre sont traitées.

Ordre des règles de filtre

IMPORTANT :

Veuillez noter la manière dont le Compliance Filter s'intègre dans l'ordre de nos services (voir Ordre des règles dans tous les services à la page 451). Dès qu'une règle d'un service s'applique à un courriel, le traitement des autres règles est interrompu. Aucune autre règle n'est appliquée au courriel.

Sur la base de cet ordre, vous pouvez créer des exceptions pour le Content Control avec des règles de filtre du Compliance Filter qui catégorisent les courriels comme **Valide**.

Les règles de filtre de Compliance Filter (voir À propos du Compliance Filter à la page 487) sont élaborées en fonction de leur type (voir Types de règles de filtre à la page 511) dans l'ordre suivant :

1. **Corps**
2. **En-tête**
3. **Avancé**

Illustration 377 : Ordre des règles de filtre en fonction du type

Les règles de filtre du même type sont classés dans en fonction de leur priorité et traités dans cet ordre.

REMARQUE :

Plus le nombre est élevé, moins la règle de filtre est prioritaire.

Les administrateurs côté clients peuvent modifier la priorité d'une règle de filtre (voir Modifier la priorité d' une règle de filtre à la page 519).

Les exemples suivants illustrent l'ordre de traitement des règles.

Élaboration simple des règles de filtre

Situation initiale :

Un administrateur côté client a défini les règles de filtre pour le Compliance Filter. Aucune règle des autres services ne s'applique à l'exemple.

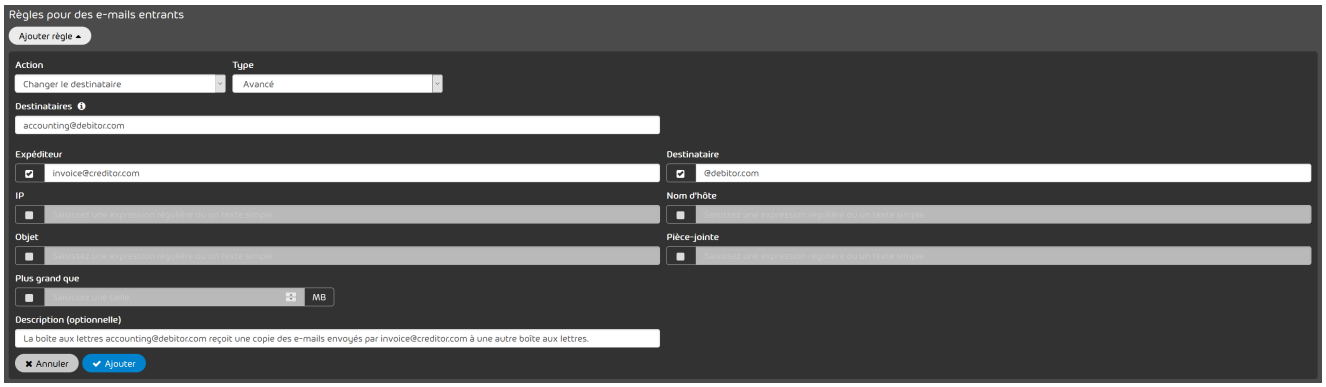


Illustration 378 : Règle de filtre : transférer

Déroulement :

1. Un courriel de **invoice@creditor.com** est envoyé à un utilisateur au choix du domaine debitor.com.
2. Le Compliance Filter parcourt d'abord les règles de filtre du type **Corps**, puis les règles de filtre du type **En-tête** et obtient un résultat dans les règles de filtre du type **Avancé**.
3. La règle de filtre est appliquée. Le Compliance Filter ne recherche pas d'autres correspondances avec d'autres règles de filtre.

Conflit entre plusieurs règles de filtre du même type

Situation initiale :

Un administrateur côté client a défini pour le Compliance Filter deux règles de filtre différentes avec le type **Avancé** au cas où un courriel sortant est envoyé à **sales@creditor.com**. Les deux règles de filtre déterminent qu'un destinataire BCC est ajouté au courriel. Pour l'une des règles de filtre, **purchasing@creditor.com** est défini comme destinataire BCC, et pour l'autre **ceo@creditor.com**. La règle de filtre avec le destinataire BCC **purchasing@creditor.com** a une priorité supérieure à celle de la règle de filtre avec le destinataire BCC **ceo@creditor.com**, et se trouve dans l'aperçu des règles de filtre, au-dessus de l'autre règle de filtre. Aucune autre règle de filtre ne s'applique à l'exemple.

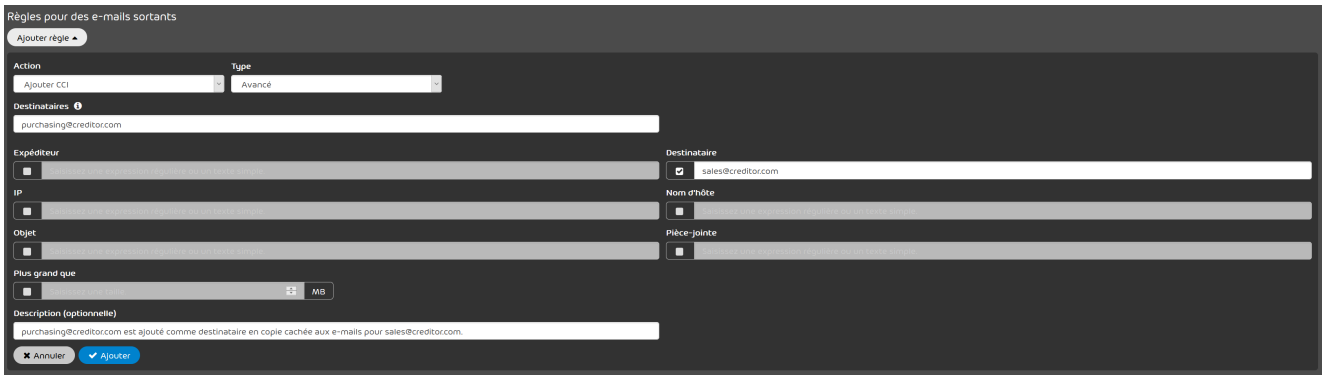


Illustration 379 : Règle de filtre : ajouter purchasing@creditor.com comme destinataire BCC

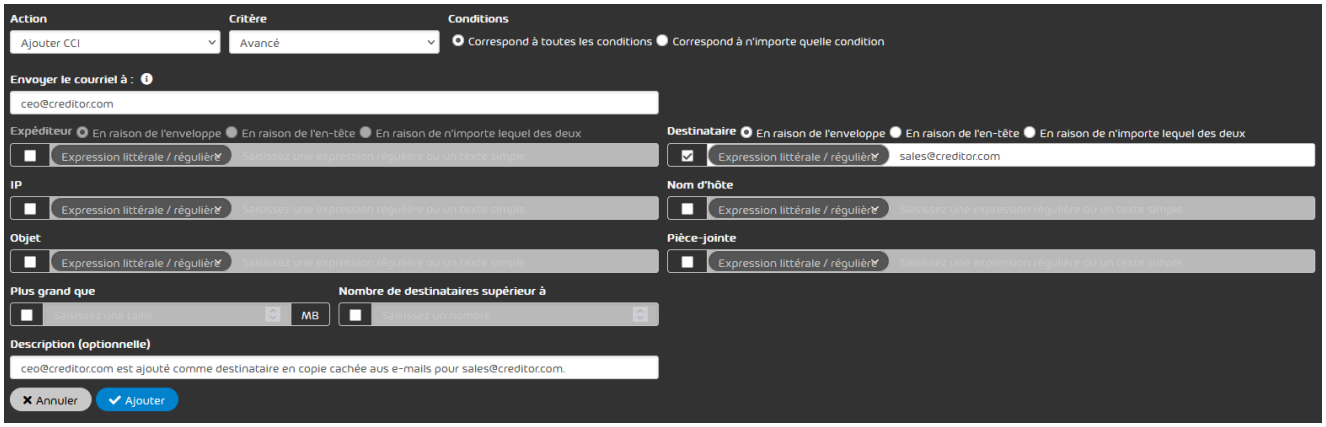


Illustration 380 : Règle de filtre : ajouter ceo@creditor.com comme destinataire BCC

Priorité	Actif	Action	Type	Conditions	Description	ID
0	☑	Ajouter CCI	Avancé	*Destinataire*: sales@creditor.com	purchasing@creditor.com est ajouté comme destinataire en copie cachée aux e-mails pour sa...	1215021
1	☑	Ajouter CCI	Avancé	*Destinataire*: sales@creditor.com	ceo@creditor.com est ajouté comme destinataire en copie cachée aux e-mail pour sales@cre...	1215001

Illustration 381 : Ordre des règles de filtre

Déroulement :

1. Un courriel d'un expéditeur quelconque est envoyé à **sales@creditor.com**.
2. Le Compliance Filter parcourt d'abord les règles de filtre du type **Corps**, puis les règles de filtre du type **En-tête** et obtient un résultat dans les règles de filtre du type **Avancé**.

3. La règle de filtre avec la priorité supérieure (BCC à **purchasing@creditor.com**) est appliquée. Le Compliance Filter ne recherche pas d'autres correspondances avec d'autres règles de filtre. La règle de filtre avec la priorité inférieure (BCC à **ceo@creditor.com**) n'est pas appliquée.

Conflit entre des règles de types différents

Situation initiale :

Un administrateur côté client a défini une règle de filtre pour que les courriels entrants avec un lien vers Facebook soient classés comme **Spam**. Dans une autre règle de filtre, l'administrateur a défini une exception pour le destinataire **marketing@debitor.com**. L'administrateur a défini comme exception que les courriels envoyés directement par Facebook à **marketing@debitor.com** soient classés comme **Valide**. La règle de filtre avec l'exception pour **marketing@debitor.com** a une priorité supérieure à celle de la règle de filtre pour les courriels avec des liens vers Facebook, et se trouve dans l'aperçu des règles de filtre, au-dessus de l'autre règle de filtre. Aucune autre règle de filtre ne s'applique à l'exemple.

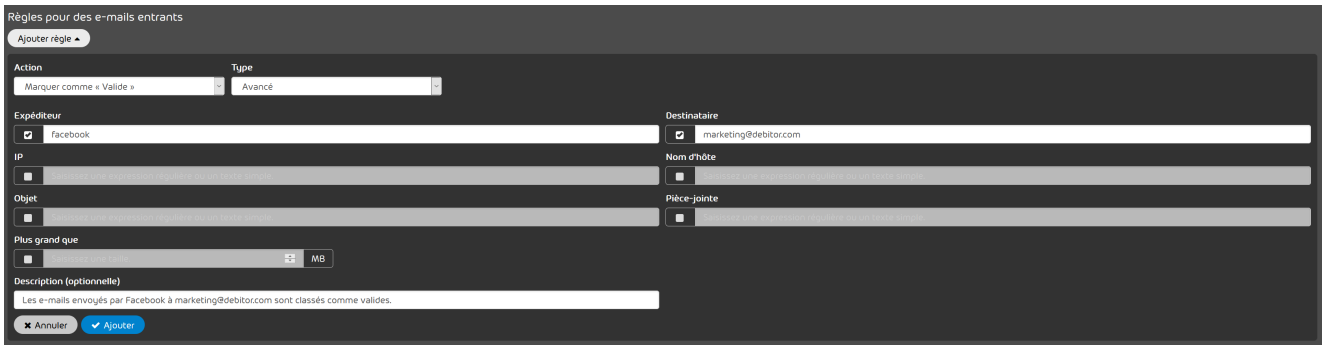


Illustration 382 : Règle de filtre : classer comme valide

Illustration 383 : Règle de filtre : classer comme courriel indésirable

Priorité	Actif	Action	Type	Conditions	Description	ID
0	☑	Marquer comme « Valide »	Avancé	*Expéditeur:* facebook; *Destinataire:* marketing@debitor.com	Les e-mails envoyés par Facebook à marketing@debitor.com sont classés comme valides.	1215121
1	☑	Marquer comme « Spam »	Corps	*Filtre: corps:* https?.*facebook	Les e-mails contenant des liens vers Facebook sont classés comme spam.	1215201

Illustration 384 : Ordre des règles de filtre

Déroulement :

1. Facebook envoie à **marketing@debitor.com** un courriel contenant un lien.
2. Le Compliance Filter parcourt d'abord les règles de filtre du type **Corps** et obtient un résultat avec la règle de filtre pour les courriels contenant des liens de Facebook.
3. La règle de filtre est appliquée au courriel et le courriel est classé comme **Spam**. Le Compliance Filter ne recherche pas d'autres correspondances avec d'autres règles de filtre. La règle de filtre avec l'exception pour **marketing@debitor.com** n'est pas appliquée malgré sa priorité supérieure, parce que les règles de filtre du type **Corps** sont prioritaires sur les autres types.

Conflit entre le Compliance Filter et nos règles de filtre

Situation initiale :

Puisque de plus en plus de spams sont envoyés à partir d'une adresse IPv4, un administrateur côté client a défini une règle de filtre pour marquer les courriels provenant de cette adresse IP comme spam. Aucune autre règle de filtre du Compliance Filter ne s'applique à l'exemple. Outre les règles de filtre du Compliance Filter, l'une des règles de filtre que nous avons définies s'applique à l'exemple.

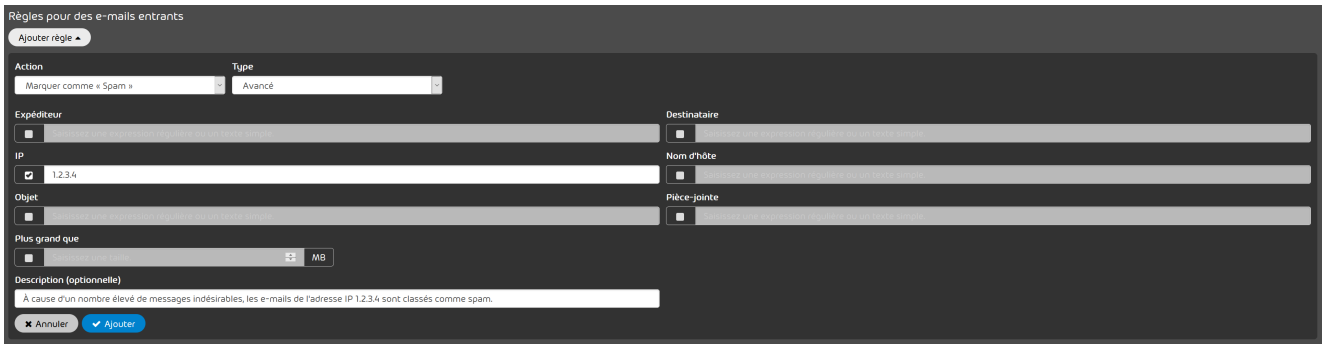


Illustration 385 : Règle de filtre : Marquer des courriels d' une adresse IPv4 définie comme spam

Déroulement :

1. Un expéditeur du domaine derrière l'adresse IPv4 envoie un courriel à un destinataire quelconque.
2. Le Compliance Filter parcourt d'abord les règles de filtre du type **Corps**, puis les règles de filtre du type **En-tête** et obtient un résultat dans les règles de filtre du type **Avancé**.
3. La règle de filtre est appliquée au courriel et le courriel est classé comme **Spam**. Le Compliance Filter ne recherche pas d'autres correspondances avec d'autres règles de filtre.
4. Nous avons déjà défini une règle de filtre plus précise pour cet exemple. Le volume accru de messages indésirables pourrait être limité à l'expéditeur **info@**. Les autres adresses courriel du domaine n'entraînent pas de courriel indésirable. Comme nos règles de filtre ne sont pas parcourues, la règle de filtre que l'administrateur côté client a définie s'applique avec une zone de validité trop grande. Ainsi, un courriel valide pourrait être classé comme courriel indésirable.

Activer une règle de filtre

Vous avez désactivé une règle de filtre du Compliance Filter (voir Désactiver une règle de filtre du Compliance Filter à la page 528).

Dès que vous souhaitez appliquer à nouveau une règle de filtre désactivée du Compliance Filter (voir À propos du Compliance Filter à la page 487), vous pouvez activer la règle de filtre dans le module **Paramètres de sécurité** > **Compliance Filter**.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.
5. Sélectionnez la règle de filtre souhaitée dans la liste des règles de filtre applicables aux courriels entrants ou sortants et activez la case à cocher dans la colonne **Actif**.

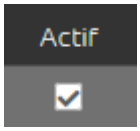


Illustration 386 : Activer la règle de filtre

La règle de filtre est activée. La règle de filtre est à nouveau appliquée au trafic de courriels du domaine.

Une règle de filtre du Compliance Filter a été activée.

Désactiver une règle de filtre du Compliance Filter

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491) et créé des règles de filtre pour le Compliance Filter (voir Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499).

Si vous souhaitez temporairement ne pas appliquer une règle de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487), vous pouvez la désactiver dans le module **Paramètres de sécurité** > **Compliance Filter**.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.

3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.
5. Sélectionnez la règle souhaitée dans la liste des règles de filtre applicables aux courriels entrants ou sortants et désactivez la case à cocher dans la colonne **Actif**.

Illustration 387 : Désactiver la règle de filtre

La règle de filtre est désactivée. La règle de filtre n'est plus appliquée au trafic de messagerie du domaine.

Une règle de filtre du Compliance Filter a été désactivée.

Vous pouvez ensuite réactiver la règle de filtre dès que celle-ci doit à nouveau être appliquée (voir Activer une règle de filtre à la page 527).

Supprimer une règle de filtre du Compliance Filter

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491) et créé des règles de filtre pour le Compliance Filter (voir Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez supprimer les règles de filtre du Compliance Filter dont vous n'avez plus besoin.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer une règle de filtre.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Règles**.

5. Dans la liste des règles pour les courriels entrants ou sortants, cliquez sur la flèche du menu à côté de la règle de filtre que vous souhaitez supprimer.

Illustration 388 : Ouvrir le menu

Un menu s'ouvre.

6. Cliquez sur **Supprimer**.

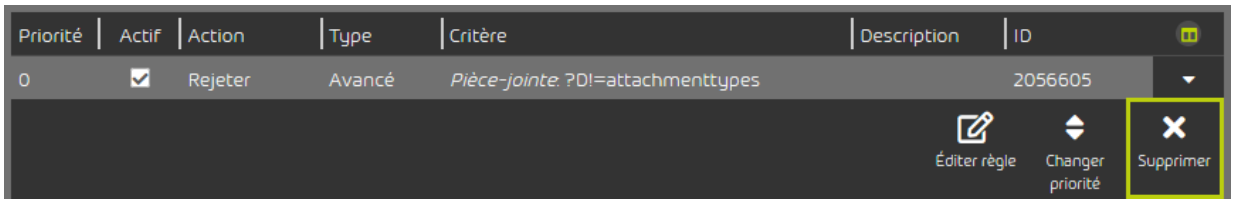


Illustration 389 : Supprimer la règle de filtre

Un message d'avertissement apparaît.

7. Cliquez sur **Confirmer**.

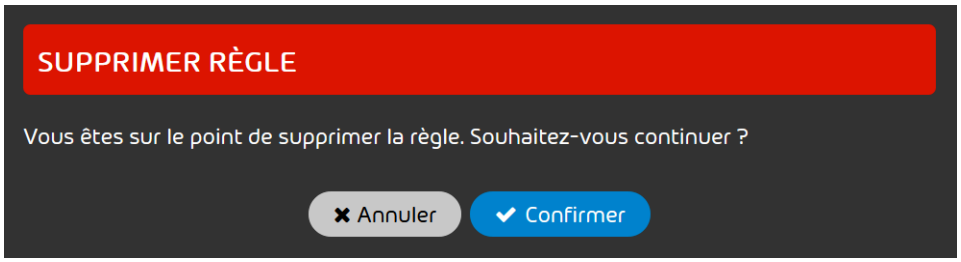


Illustration 390 : Confirmer la suppression

La règle de filtre est supprimée.

Une règle de filtre du Compliance Filter a été supprimée.

Dictionnaires

Les dictionnaires sont des collections d'expressions qui peuvent être utilisées pour créer des règles de filtre dans le module **Paramètres de sécurité** > **Compliance Filter** (voir À propos du Compliance Filter à la page 487). Les expressions d'un dictionnaire peuvent être interprétées soit comme des expressions littérales, soit comme des expressions régulières. Les expressions régulières offrent une meilleure précision et réduisent le nombre d'entrées à créer et à gérer.

REMARQUE :

Il est possible de créer jusqu'à 250 dictionnaires pour un domaine principal.

Les dictionnaires qui contiennent des expressions régulières peuvent contenir jusqu'à 1000 entrées, tandis que les dictionnaires qui contiennent des expressions littérales peuvent contenir jusqu'à 15000 entrées.

Lors de la création des règles de filtre du type **Avancé** (voir Créer une règle de filtre pour les courriels entrants à la page 493 ou Créer une règle de filtre pour les courriels sortants à la page 499), les administrateurs côté clients peuvent, à certaines conditions, référencer un dictionnaire au lieu de saisir une seule expression. Pour référencer un dictionnaire existant, les administrateurs doivent saisir le nom du dictionnaire dans le champ de saisie de la condition et choisir dans un menu déroulant comment les expressions du dictionnaire doivent être interprétées par la règle de filtre. L'option **Figure dans le dictionnaire** permet que la règle de filtre s'applique si au moins une expression du dictionnaire correspond à un courriel. Les expressions du dictionnaire sont donc logiquement liées entre elles par un OU à l'intérieur de la condition. L'option **Ne figure pas dans le dictionnaire** permet que la règle de filtre s'applique si aucune correspondance n'est trouvée pour une expression.

Les dictionnaires simplifient la création des règles de filtre du Compliance Filter, car une seule règle de filtre peut s'appliquer à des courriels qui ont des valeurs différentes pour une condition. Par exemple, une seule règle de filtre permet de marquer comme valides les courriels des expéditeurs **@facebook**, **@instagram** ou **@tiktok** envoyés à des adresses courriel du département marketing en créant un dictionnaire contenant les trois termes et en les référençant dans la condition **Expéditeur** (voir Types de règles de filtre à la page 511). Pour obtenir le même comportement du Compliance Filter sans référence à un dictionnaire, il faudrait soit trois règles de filtre différentes,

chacune ayant une expression littérale pour un expéditeur, soit une seule règle de filtre avec une expression régulière avec des liens OU entre les différents expéditeurs. Cette dernière risque d'être complexe si le nombre d'expéditeurs enregistrés est important.

Un autre cas d'utilisation consiste à rejeter tous les courriels entrants qui contiennent des jurons. Pour ce faire, un administrateur côté client pourrait créer un dictionnaire contenant des jurons et le référencer dans une règle de filtre pour les courriels entrants. Le fait de créer et de maintenir des règles de filtre individuelles pour chaque juron serait en revanche nettement plus fastidieux.

Les administrateurs côté clients peuvent créer des dictionnaires (voir Créer un dictionnaire à la page 532), éditer des dictionnaires existants (voir Éditer un dictionnaire à la page 535) et en supprimer (voir Supprimer un dictionnaire à la page 537).

Créer un dictionnaire

Vous avez activé le Compliance Filter pour le domaine sélectionné (voir Activer le Compliance Filter à la page 491).

Le module **Compliance Filter** > **Dictionnaires** vous permet de créer des dictionnaires (voir Dictionnaires à la page 531) pour le Compliance Filter. Les dictionnaires permettent de créer facilement des règles de filtre complexes (voir Créer une règle de filtre pour les courriels entrants à la page 493 et Créer une règle de filtre pour les courriels sortants à la page 499).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer un dictionnaire.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Dictionnaires**.

5. Cliquez sur **Ajouter**.

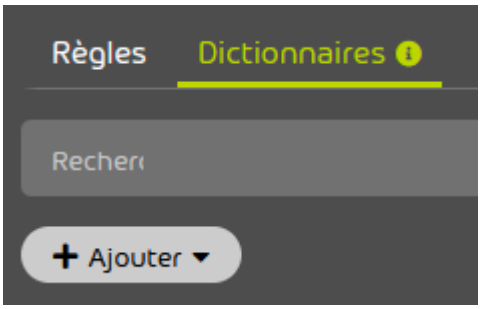


Illustration 391 : Ajouter un dictionnaire

Un formulaire de création de dictionnaire apparaît.

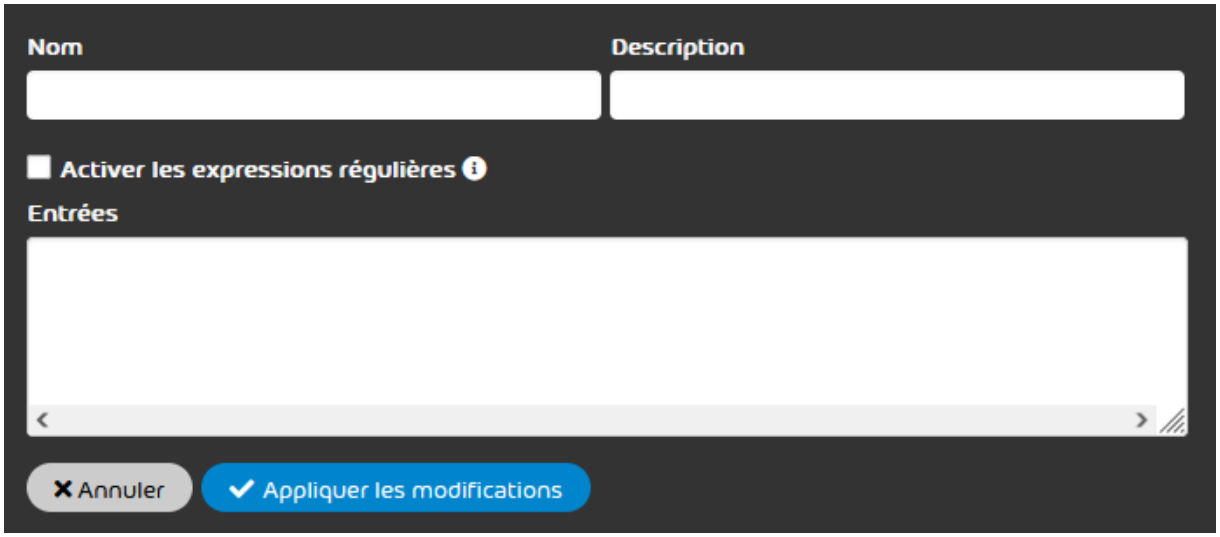


Illustration 392 : Formulaire pour un dictionnaire

6. Dans le champ **Nom**, saisissez un nom pour le dictionnaire.

> **REMARQUE :**
>
> Le nom peut contenir les caractères suivants :
>
> - Lettres latines minuscules de a à z
> - Chiffres de 0 à 9
> - Caractères spéciaux **- _ . , =**
>
> Les espaces et les deux points ne sont pas autorisés.

7. Facultatif : Dans le champ **Description**, saisissez une description du dictionnaire.
8. Facultatif : Si les entrées du dictionnaire doivent être interprétées comme des expressions régulières, cochez la case **Activer les expressions régulières**.

> **REMARQUE :**
>
> Si cette option est sélectionnée, les règles des expressions régulières (voir Explication des expressions régulières à la page 541) ainsi que leurs exceptions (voir Exceptions pour les expressions régulières à la page 549) doivent être respectées pour toutes les entrées du dictionnaire.

9. Dans le champ **Entrées**, saisissez les expressions souhaitées.

> **REMARQUE :**
>
> Chaque ligne correspond à une entrée. La longueur maximale des lignes est de 1000 caractères. Le nombre d'entrées est limité à 15 000 pour les expressions littérales et à 1000 pour les expressions régulières. Les lignes vides et les doublons sont ignorés et supprimés lors de l'enregistrement du dictionnaire.

10. Cliquez sur **Appliquer les modifications**.

Si la case **Activer les expressions régulières** est cochée, il est vérifié si les expressions régulières sont correctes.

Le formulaire se ferme, le dictionnaire est enregistré et ajouté au tableau des dictionnaires.

Un dictionnaire a été créé.

Vous pouvez ensuite modifier (voir Éditer un dictionnaire à la page 535) ou supprimer (voir Supprimer un dictionnaire à la page 537) le dictionnaire. Vous pouvez référencer le dictionnaire dans les règles de filtre du Compliance Filter (voir Créer une règle de filtre pour les courriels entrants à la page 493 et Créer une règle de filtre pour les courriels sortants à la page 499).

Éditer un dictionnaire

Vous avez créé un dictionnaire (voir Créer un dictionnaire à la page 532).

Dans le module **Paramètres de sécurité** > **Compliance Filter**, vous pouvez modifier les dictionnaires existants (voir Dictionnaires à la page 531) du Compliance Filter (voir À propos du Compliance Filter à la page 487).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez modifier un dictionnaire.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Dictionnaires**.
5. Dans la liste des dictionnaires, cliquez sur la flèche de menu à côté du dictionnaire que vous souhaitez modifier.

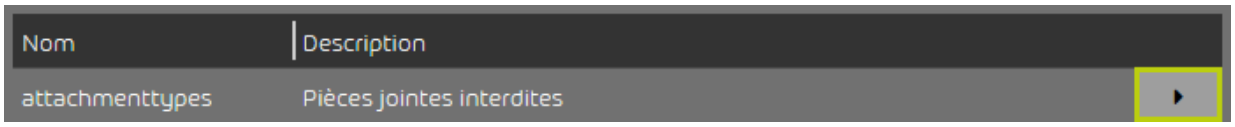


Illustration 393 : Ouvrir le menu

6. Cliquez sur **Éditer**.

Illustration 394 : Modifier le dictionnaire

Un formulaire avec les paramètres actuels du dictionnaire s'ouvre.

7. Modifiez les paramètres en fonction de vos besoins.

REMARQUE :

Pour de plus amples informations, voir Créer un dictionnaire à la page 532.

8. Cliquez sur **Appliquer les modifications**.

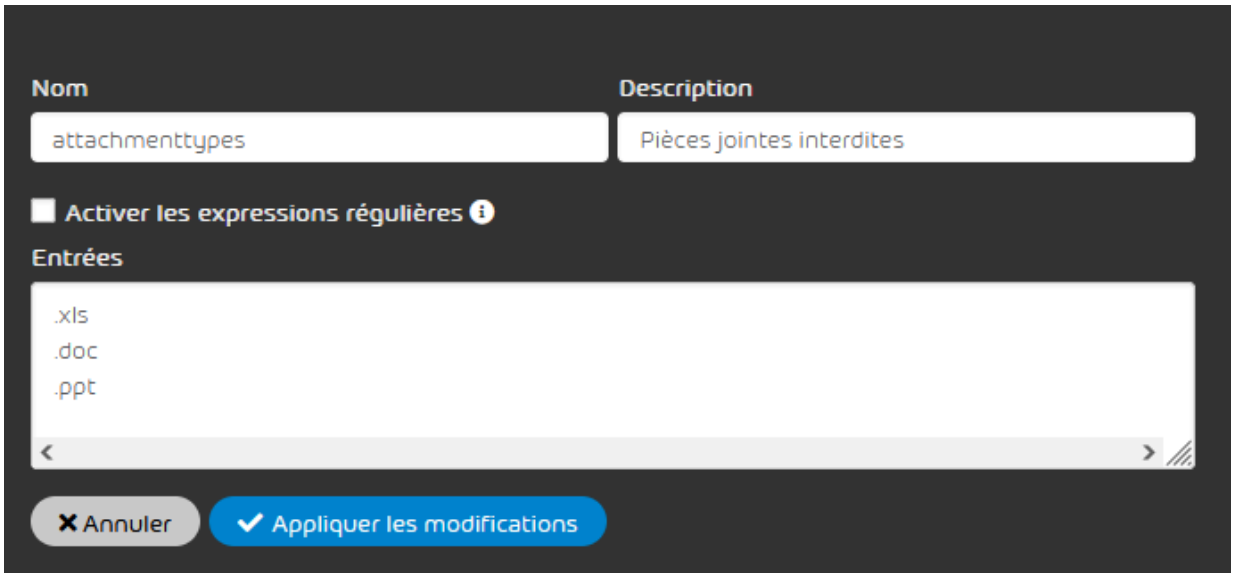


Illustration 395 : Appliquer les modifications

Les modifications sont acceptées.

REMARQUE :

Si le nom du dictionnaire a été modifié et que le dictionnaire est déjà référencé dans des règles de filtre, le nom du dictionnaire est également mis à jour dans ces règles de filtre.

Un dictionnaire a été modifié.

Supprimer un dictionnaire

Vous avez créé un dictionnaire (voir Créer un dictionnaire à la page 532). Le dictionnaire n'est référencé dans aucune règle de filtre du Compliance Filter.

Si vous n'avez plus besoin d'un dictionnaire existant (voir Dictionnaires à la page 531) du Compliance Filter (voir À propos du Compliance Filter à la page 487), vous pouvez le supprimer dans le module **Paramètres de sécurité** > **Compliance Filter**.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez supprimer un dictionnaire.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Sélectionnez l'onglet **Dictionnaires**.
5. Dans la liste des dictionnaires, cliquez sur la flèche de menu à côté du dictionnaire que vous souhaitez supprimer.

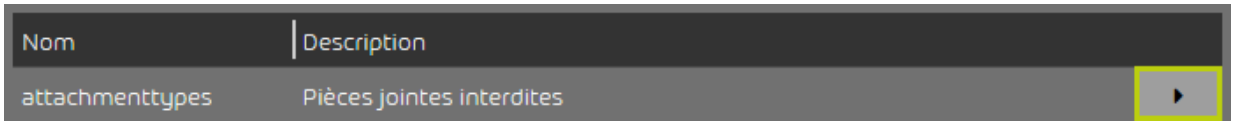


Illustration 396 : Ouvrir le menu

- Un menu s'ouvre.

6. Cliquez sur **Supprimer**.

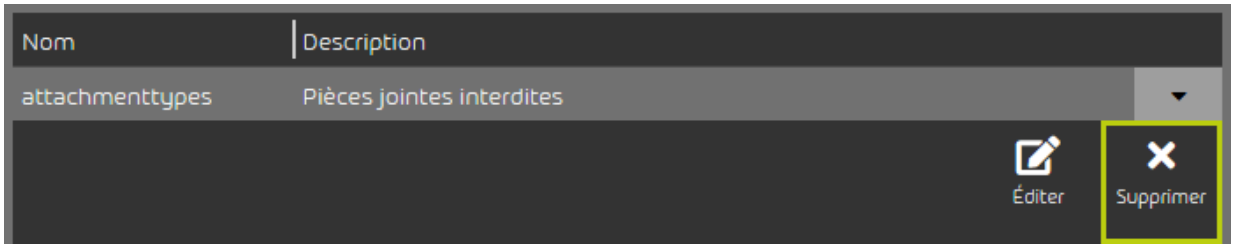


Illustration 397 : Supprimer le dictionnaire

- Un message d'avertissement apparaît.

7. Cliquez sur **Confirmer**.

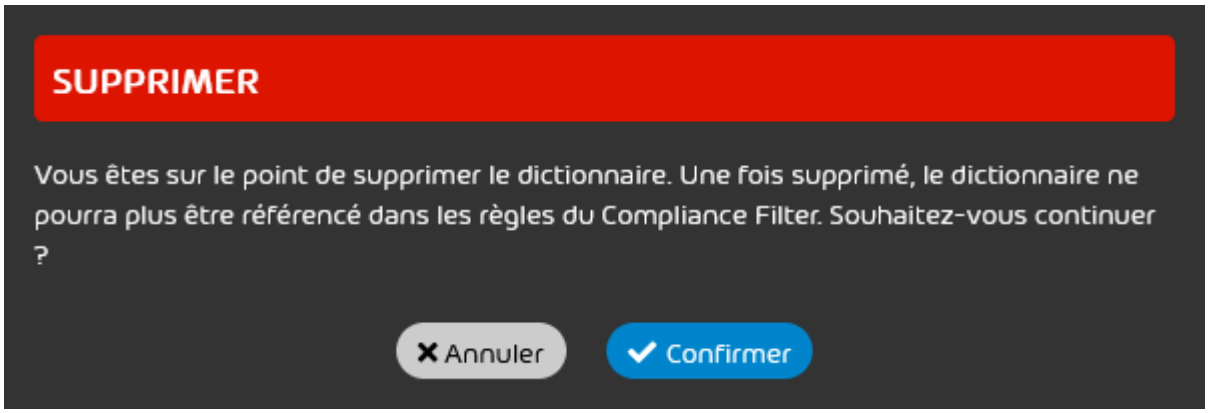


Illustration 398 : Confirmer la suppression

Il est vérifié si le dictionnaire est référencé dans les règles de filtre du Compliance Filter. S'il n'est pas référencé, le dictionnaire sera supprimé.

Un dictionnaire a été supprimé.

Expressions régulières

Dans les règles de filtre du Compliance Filter (voir Règles de filtre à la page 492), des expressions régulières (RegEx en abrégé) peuvent être utilisées pour extraire des informations à partir d'une chaîne de caractères Il est ainsi possible de détecter des motifs récurrents dans les lignes d'objet ou d'autres composants des courriels et de filtrer les courriels.

REMARQUE :

Le système place automatiquement la séquence **.*** au début et à la fin des expressions régulières du module **Compliance Filter**, à moins que l'expression régulière ne commence par **^** ou ne se termine par **$**.

REMARQUE :

Les quantificateurs **+** et ***** (voir le tableau Éléments de syntaxe et caractères spéciaux au chapitre Explication des expressions régulières à la page 541) sont automatiquement rendus inertes lorsqu'un point d'interrogation est placé après ceux-ci, et ce, avant que les expressions régulières ne soient évaluées.

« Inerte » est le contraire d' « avide » et signifie que la recherche se termine par la correspondance la plus courte possible. Par exemple, l'expression régulière avide **a.*b** trouverait dans la chaîne de caractères **aabcaabcdf** la correspondance **aabcaab**. L'expression inerte **a.*?b**, quant à elle, trouverait deux fois la correspondance **aab** dans la même chaîne de caractères.

IMPORTANT :

Dans le module **Compliance Filter**, les expressions régulières peuvent uniquement être utilisées dans les règles de filtre de type **Avancé** (voir Types de règles de filtre à la page 511) et dans les dictionnaires (voir Dictionnaires à la page 531).

Pour obtenir une explication sur les expressions régulières ainsi que des exemples d'expressions régulières, voir Explication des expressions régulières à la page 541 et Exemples d' expressions régulières complexes à la page 552.

Dans le Compliance Filter, des expressions régulières peuvent être créées selon les Perl Compatible Regular Expressions. Les autres bibliothèques ne sont pas prises en charge. Vous trouverez de plus amples informations sur : http://www.pcre.org/. En outre, il existe des restrictions spéciales, qui sont expliquées sous Exceptions pour les expressions régulières à la page 549.

Exemple : utilisation d' expressions régulières dans le Compliance Filter

Les utilisateurs recevaient souvent des courriels dont le sujet contenait le mot « porn ». Une règle de filtrage a été définie pour les marquer comme courriel indésirable. Récemment, cependant, il y a eu une augmentation du nombre de courriels utilisant Leetspeak pour contourner ce filtre. Par exemple, les courriels dont l'objet est « p0rn » sont reçus et qui ne sont pas marqués par le Compliance Filter. Dans ce cas, l'utilisation d'une expression régulière est plus efficace :

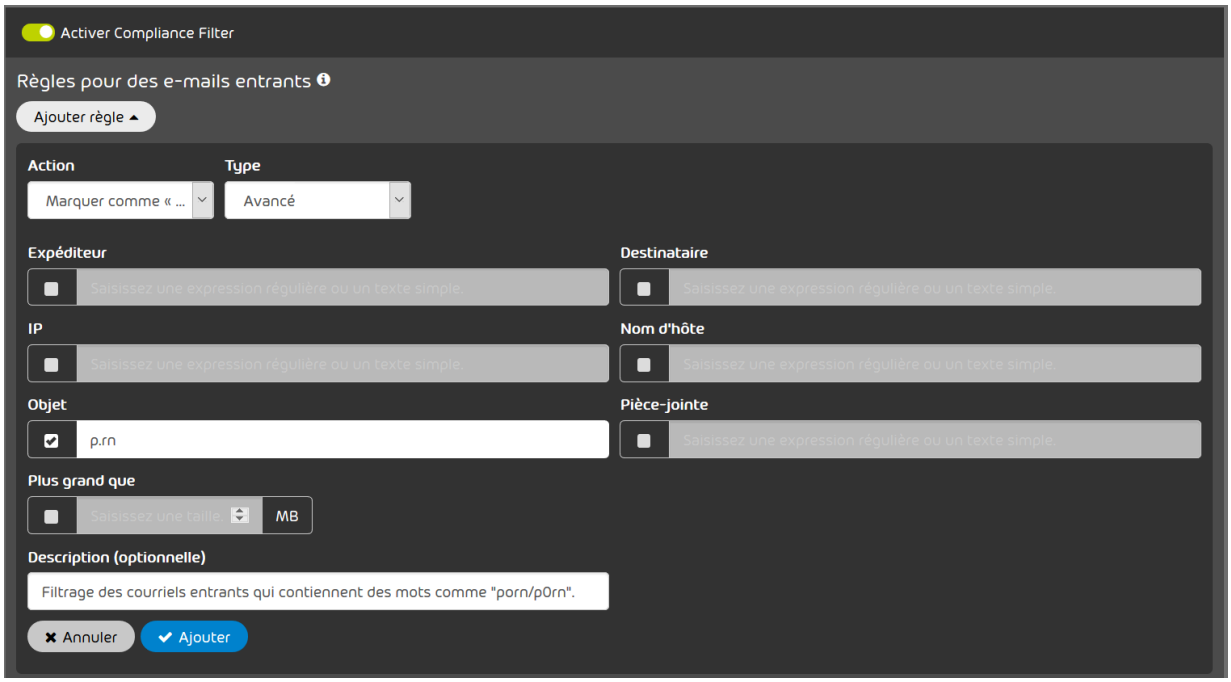


Illustration 399 : Utilisation d' une expression régulière dans le Compliance Filter

À la place du point, chaque caractère est interprété comme valide. À ce stade, le filtre n'est plus seulement réglé sur « o », mais réagit également à toutes les lettres, chiffres et caractères spéciaux.

Explication des expressions régulières

Dans les exemples d'expressions régulières suivants, les expressions régulières sont formées dans la colonne de droite et appliquées aux textes de la colonne de gauche. La sélection indique la partie du texte qui a été détectée par l'expression régulière.

Caractères individuels

Tableau 31 : Saisir des lettres

TEXTE	REGEX
abcdef	**abc**

TEXTE	REGEX
abcde	
Abcd	

Avec les lettres, les occurrences correspondantes peuvent être recherchées n'importe où dans le texte.

Tableau 32 : Saisir des caractères à partir de la sélection de caractères

TEXTE	REGEX
ac**bde**f	**[abc]de**
adefg	

Une sélection de caractères permet de rechercher l'un des caractères regroupés entre crochets pour former une sélection.

Tableau 33 : Saisir des caractères à partir des plages de caractères

TEXTE	REGEX
1 Mot	**[1-5] [A-Z]**
7 mots	
2 mots différents	

Les crochets permettent également d'indiquer des plages de caractères. Le premier et le dernier caractère de la plage sont séparés par un tiret. L'ordre des caractères correspond à l'ordre dans le tableau ASCII. Les lettres majuscules viennent donc avant les lettres minuscules. Par conséquent, l'expression régulière **[A-z]** trouve tous les caractères ASCII, de la lettre majuscule A à

la lettre minuscule z. L'expression régulière **[a-Z]** quant à elle n'est pas valide et ne trouve aucune correspondance.

> **IMPORTANT :**
>
> La plage de caractères **[A-z]** ne contient que des lettres latines. Les caractères suivants ne sont pas compris dans la plage de caractères :
>
> - Voyelles infléchies (äöü)
> - Lettres avec accents (par exemple áéíóú)
> - Lettres spécifiques à une langue (par exemple ñ ou ß)

Tableau 34 : Saisir des chiffres

TEXTE	REGEX
number - **123**	**123** ou **\d\d\d**
var number - **123**	
ab**123**fg	

Les chiffres ont le même effet que les lettres. Il est possible d'utiliser la classe de caractères **\d** au lieu d'un nombre explicite pour obtenir un résultat sur n'importe quel nombre.

Tableau 35 : Saisir des lettres

TEXTE	REGEX
a12**b**34**c**	**\w**

L'expression **\w** recherche n'importe quel lettre latine de A à z (voir plus haut), sans caractères spéciaux ni lettres spécifiques à une langue.

Tableau 36 : Saisir n’ importe quel caractère

TEXTE	REGEX
bob.	···\.
tom.	
?!a.	
abc1	

Le « . » simple exprime que chaque caractère génère un résultat. Pour vérifier l'occurrence d'un point, le point doit être masqué avec « \. ».

Tableau 37 : Saisir plusieurs fois les caractères

TEXTE	REGEX
abcc	**ab*c**
a**abbbbbc**c	
bb**ac**cc	

Répétitions

L'astérisque qui suit signifie que le caractère précédent peut être utilisé aussi souvent que souhaité. Le caractère peut donc ne pas apparaître du tout, apparaître une fois ou plusieurs fois.

Tableau 38 : Saisir les caractères au moins une fois

TEXTE	REGEX
aaaaaaaaa**abc**	**ab+c**
a**abbbc**	
ac	

Le signe « plus » signifie que le caractère doit survenir au moins une fois et qu'il peut survenir plusieurs fois. Cela ne se produit pas lorsqu'aucun résultat n'est trouvé.

Tableau 39 : Déterminer le nombre de répétitions des caractères

TEXTE	REGEX
12 **123 4544 1564**14	**\d{3,4}**

Il est possible d'indiquer entre accolades un nombre fixe ou un intervalle pour le nombre de répétitions du caractère qui précède. L'exemple ci-dessus montre une recherche des chaînes de caractères composées uniquement de chiffres et d'une longueur de 3 à 4 caractères. Les combinaisons suivantes sont possibles :

- {m} : le caractère qui précède doit apparaître exactement m fois.
- {m,} : le caractère qui précède doit apparaître au moins m fois.
- {m,n} : le caractère qui précède doit apparaître au moins m fois et au maximum n fois.

Tableau 40 : Caractères en option

TEXTE	REGEX
3 users online	**\d+ users? online**
150 users online	

TEXTE	REGEX
20 users online	
1 user online	
no user online	

Un « ? » en suffixe sélectionne le caractère placé devant comme optionnel.

Groupes

Tableau 41 : Répartir l’ expression régulière en groupes

TEXTE	REGEX
dump025.csv	**\w+\d+\.(\w+)**
dump026.csv	

Les parenthèses autour d'une partie de l'expression régulière déclenchent des groupes. Dans l'exemple ci-dessus, l'extension de fichier après le point est enregistrée comme un groupe. Les groupes sont traités comme des caractères individuels par différents opérateurs. Les quantificateurs qui précèdent, tels que ?, *, + ou les accolades ont donc un effet sur le groupe dans son ensemble et pas seulement sur le dernier caractère. Le groupe **(abc)?** entier serait par exemple une option. En outre, les groupes permettent d'effectuer des opérations avancées, telles de que la référence arrière (voir ci-après). Un autre avantage est que les groupes améliorent la clarté.

Tableau 42 : Soit ou sélection

TEXTE	REGEX
data.csv	**.*\.(exe|xlsx)**
bild.jpg	

TEXTE	REGEX
moving.gif	
document.pdf	
virus.exe	
locky.xlsx	

Les chaînes de caractères à rechercher sont séparées l'une de l'autre par un trait vertical | entre parenthèses.

Tableau 43 : Référence arrière

TEXTE	REGEX
From: "local@domain.de" <local@domain.de>	**From: "(.*@.*\.de)" <\1>**
From: "local@domain.de" <hacker@hackeddomain.de>	

La référence arrière \1 prend la définition du groupe (.*@.*\.de). Un seul résultat est généré si le résultat du groupe se produit à nouveau à la position de référence.

Éléments de syntaxe et caractères spéciaux

Les éléments syntaxiques suivants sont autorisés pour la construction d'expressions régulières dans le Compliance Filter :

Tableau 44 : Éléments syntaxiques

CARACTÈRE DE REMPLACEMENT/CLASSE DE CARACTÈRES	FONCTION
abc…	Lettres
123…	Chiffres
[abc]	Un des caractères a, b ou c
[a-z]	Un des caractères ASCII dans la plage indiquée
\d	Chaque chiffre
.	Chaque caractère
\. \/ \ *	Masque des caractères en gras
\w	Chaque caractère alphanumérique
*	0 ou plus de répétitions de l'expression qui précède
+	1 ou plus de répétitions de l'expression qui précède
?	L'expression qui précède est facultative
{m}	Exactement m répétitions de l'expression qui précède
{m,}	Au moins m répétitions de l'expression qui précède
{m, n}	m à n répétitions de l'expression qui précède

CARACTÈRE DE REMPLACEMENT/CLASSE DE CARACTÈRES	FONCTION
\s	Chaque espace
(...)	Groupe d'extraction
(.*)	Tout
(abc|def)	abc ou def
^	Début de la chaîne de caractères
$	Fin de la chaîne de caractères

Les caractères spéciaux du tableau ci-dessus sont interprétés par défaut comme faisant partie d'une expression régulière. Cependant, il est également possible de rechercher ces caractères spéciaux littéralement. Pour cela, les fonctions de ces caractères spéciaux doivent être contournées en les faisant précéder d'une barre oblique inversée ****. L'expression **A***, par exemple, ne trouve pas un nombre quelconque de A, mais la chaîne de caractères littérale **a***.

Exceptions pour les expressions régulières

La création d'expressions régulières pour le Compliance Filter (voir À propos du Compliance Filter à la page 487 et Règles de filtre à la page 492) diffère des expressions conformes PCRE car tous les éléments syntaxiques ne peuvent pas être utilisés dans le Compliance Filter. En principe, les caractères de la table ASCII étendue sont autorisés. Lors de l'examen des expressions régulières, il n'y a aucune distinction entre les majuscules et les minuscules.

Des restrictions différentes s'appliquent aux expressions qui sont directement saisies dans les champs de saisie des règles de filtre dans le module **Compliance Filter** et aux expressions dans les dictionnaires (voir Dictionnaires à la page 531).

Les caractères suivants ne peuvent **pas** être utilisés dans les champs de saisie des règles de filtre du module **Compliance Filter** dont les valeurs sont interprétées comme des expressions régulières :

- Point-virgule ;
- Degrés °
- Astérisque * au début d'une entrée
- Barre oblique / (sauf si elle est masquée par \)

Les caractères suivants ne peuvent **pas** être utilisés dans les dictionnaires du module **Compliance Filter** dont les entrées sont interprétées comme des expressions régulières :

- Degrés °
- Barre oblique / (sauf si elle est masquée par \)

REMARQUE :

Le trait vertical | (pipe) n'est autorisé, tant dans les champs de saisie des règles de filtre que dans les dictionnaires, qu'à l'intérieur d'un groupe entouré de parenthèses rondes. En outre, le trait vertical | est toujours utilisé individuellement lorsqu'il a la fonction « OU ». Deux traits verticaux || sont interprétés comme un caratère de remplacement et entraînent l'acceptation de tous les signes.

Cas d'utilisation fréquents d'expressions régulières

Des exemples d'expressions régulières (voir Explication des expressions régulières à la page 541) pour des cas d'utilisation fréquents dans le Compliance Filter (voir À propos du Compliance Filter à la page 487) sont présentés ci-après.

Noms d'hôte différents avec la même extension

Lors de la création de règles de filtre pour les courriels envoyés depuis ou vers les serveurs de messagerie de différents sous-domaines d'un certain domaine, la condition **Nom d'hôte** du module **Paramètres de sécurité** > **Compliance Filter** permet de rechercher les chaînes de caractères qui se terminent d'une certaine manière.

L'expression régulière suivante peut être utilisée pour cette recherche :

Chaîne de caractères$

Le symbole de dollar signifie que la chaîne de caractères recherchée doit être trouvée à la fin du nom d'hôte analysé. Par exemple, l'expression **.*domain\.tld$** trouverait les courriels depuis ou vers le serveur de messagerie du domaine **domain.tld** et de tous ses sous-domaines (par ex. **marketing.domain.tld**, **sales.domain.tld**, **accounting.domain.tld**).

Noms d'hôtes numérotés des serveurs de messagerie

Les différents serveurs de messagerie d'un domaine ne se distinguent souvent qu'au niveau de leur numérotation. Pour traiter les courriels de ou vers ces serveurs de messagerie par des règles de filtre du Compliance Filter, la condition **Nom d'hôte** permet de rechercher des chaînes de caractères qui ne diffèrent qu'au niveau de leur numérotation.

L'expression régulière suivante peut être utilisée pour cette recherche :

(Chaîne de caractères avant la numérotation)\d+(chaîne de caractères après numérotation)

> **REMARQUE :**
>
> Les parenthèses dans cette expression sont facultatives et ont été utilisées pour apporter plus de clarté.

La séquence **\d+** signifie « au moins un chiffre ». Par exemple, l'expression régulière **mx\d+\.domain\.tld** trouverait les courriels de ou vers des serveurs de messagerie suivants : **mx3.domain.tld**, **mx30.domain.tld**, **mx100.domain.tld**.

Plusieurs adresses courriel concrètes d'un domaine

Pour qu'une règle de filtre s'applique à un petit nombre d'adresses courriel d'un domaine, il est possible d'utiliser une expression régulière pour la condition **Expéditeur** ou **Destinataire** selon le modèle suivant :

(utilisateur1|utilisateur2|utilisateur3)@domain

Le symbole **|** sépare différentes chaînes de caractères alternatives, dont l'une doit être trouvée. Les chaînes de caractères alternatives doivent être entre parenthèses. Par exemple, l'expression régulière **(klaus|peter|petra)@domain.com** trouverait les courriels de ou vers les adresses courriel suivantes : **klaus@domain.com**, **peter@domain.com**, **petra@domain.com**.

Exemples d’ expressions régulières complexes

Enfin, nous examinons l'application d'expressions régulières complexes (voir Explication des expressions régulières à la page 541) dans le cadre de règles de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487) :

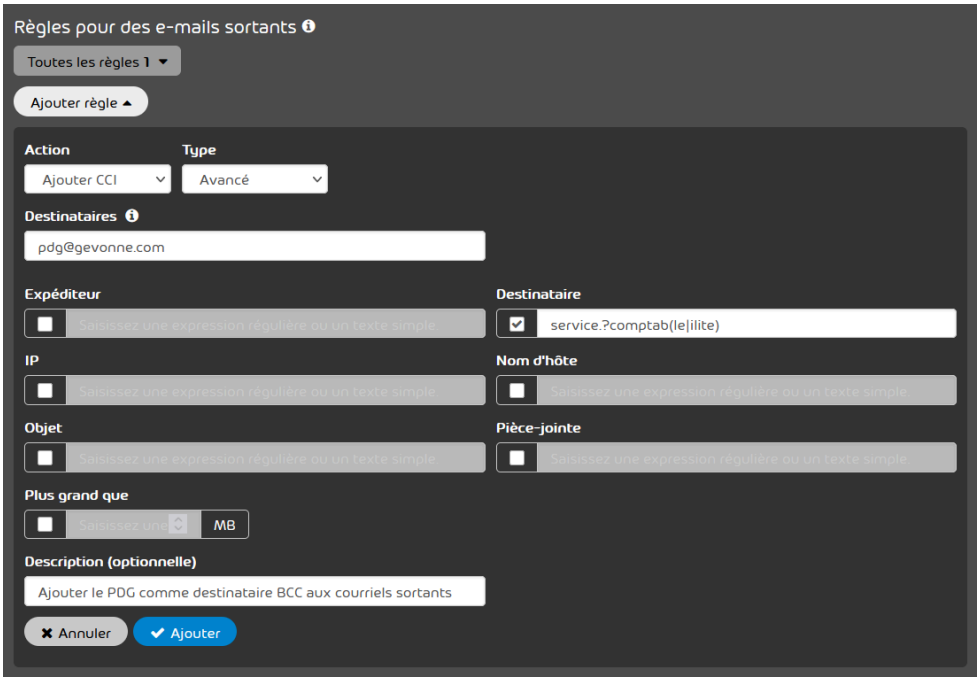


Illustration 400 : Recherche de destinataires

Dans ce premier exemple, un client souhaite que son directeur reçoive une copie cachée des courriels sortants envoyés au service de comptabilité des clients de l'entreprise. Ces adresses courriel sont établies selon un modèle précis. L'expression régulière **service.?comptab(le|ilite)** permet de saisir les segments de texte suivants et de nombreuses autres combinaisons :

- **servicecomptable@test.fr**
- **service_comptable@test.fr**
- **servicecomptabilite@test.fr**
- **servicecomptabilite@unautretest.fr**

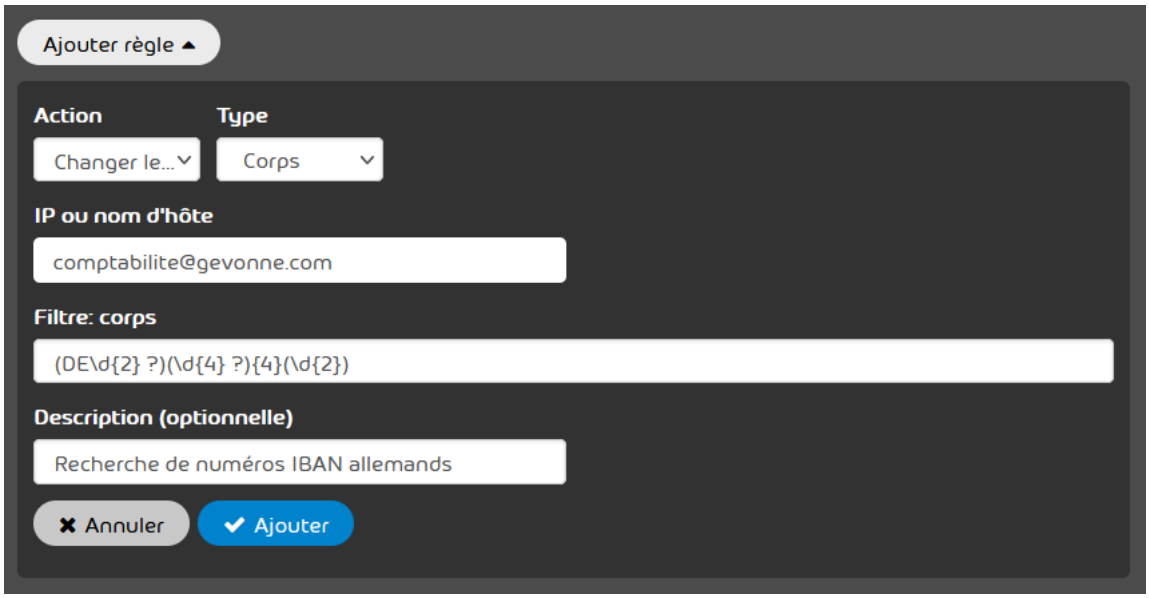


Illustration 401 : Recherche d' IBAN dans le corps du courriel

Dans cet exemple, un client souhaite transmettre à son service de comptabilité tous les courriels entrants qui contiennent des numéros de comptes IBAN allemands dans le corps du courriel. L'expression régulière **(DE\d{2} ?)(\d{4} ?){4}(\d{2})** permet de rechercher des numéros de comptes IBAN allemands. Cette expression régulière trouve aussi bien les numéros de comptes IBAN allemands sans espaces que les numéros de comptes IBAN allemands divisés en blocs de 4 caractères et un bloc final de 2 caractères, conformément à l'orthographe usuelle :

- **DE12345678901234567890**
- **DE12 3456 7890 1234 5678 90**

Désactiver le Compliance Filter

Si vous ne souhaitez plus utiliser les règles de filtre du Compliance Filter (voir À propos du Compliance Filter à la page 487), vous pouvez désactiver le Compliance Filter dans le module **Paramètres de sécurité** > **Compliance Filter**. Toutes les règles créées seront supprimées.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez désactiver le Compliance Filter.
3. Naviguez vers **Paramètres de sécurité** > **Compliance Filter**.
4. Actionnez le bouton **Activer Compliance Filter**.

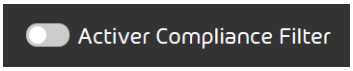


Illustration 402 : Désactiver le Compliance Filter

Une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Confirmer**.

Illustration 403 : Confirmer

Le Compliance Filter est désactivé. Toutes les règles sont supprimées. Les paramètres dans le module **Compliance Filter** sont verrouillés. Aucune autre entrée n'est possible.

Le Compliance Filter a été désactivé.

Signature and Disclaimer

À propos de Signature and Disclaimer

Signature and Disclaimer contrôle la mise à disposition automatisée et centralisée des signatures et disclaimers de courriels. Les signatures et les disclaimers peuvent être créés soit pour toutes les boîtes aux lettres d'un domaine, soit uniquement pour les boîtes aux lettres d'un groupe spécifique (voir « Groupes » dans le manuel du Control Panel). En se synchronisant Active Directory, l'outil

génère dynamiquement des signatures personnalisées basées sur un modèle précédemment créé qui sont automatiquement insérées après le texte actuel du courriel. Ainsi, les variables Active Directory (variable AD) intégrées avec les informations depuis les attributs Active Directory correspondants dans la signature ou le disclaimer sont utilisées. Pour les boîtes aux lettres qui ont été créées manuellement dans le Control Panel et qui ne sont pas synchronisées via LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel), les données de base de la boîte aux lettres sont utilisées pour les variables AD.

L'utilisation de variables AD n'est possible que pour les clients dont les utilisateurs et les groupes sont synchronisés via LDAP à partir d'un Microsoft Active Directory. Les autres services de répertoire ne sont pas pris en charge.

REMARQUE :

Les signatures et disclaimers sont ajoutés à tous les courriels qui sont envoyés via nos serveurs de relais. Par conséquent, les signatures et disclaimers sont aussi ajoutés aux courriels envoyés au sein d'une entreprise s'ils sont acheminés via notre infrastructure.

Les administrateurs côté client et les utilisateurs avec le rôle **Marketing** (voir Accès au module Signature and Disclaimer à la page 556) peuvent régler des signatures et des disclaimers. Les fonctions de Signature and Disclaimer sont également disponibles pour les téléphones portables (voir Utilisation mobile de Signature and Disclaimer à la page 556).

Le service doit être activé avant que Signature and Disclaimer ne puisse activé (voir Activer Signature and Disclaimer à la page 556). Les signatures et les clauses de non-responsabilité pour des groupes peuvent ensuite être créés dans un éditeur (voir Créer des signatures et des disclaimers à la page 558), édités ou supprimés (voir Éditer ou supprimer une signature ou un disclaimer à la page 565). La priorité des groupes peut être modifiée (voir Modifier les priorités des groupes à la page 563). Dans l'éditeur, les signatures et les disclaimers sont affichés telles qu'ils seront émis par la suite (voir Éditeur WYSIWYG à la page 568). Les graphiques peuvent également être intégrés dans les signatures et les disclaimers (voir Intégration des graphiques dans les signatures et disclaimers à la page 584). Si des signatures et des disclaimers basés sur des groupes sont créés, les priorités des groupes peuvent être modifiées (voir Modifier les priorités des groupes à la page 563).

Si vous ne souhaitez plus utiliser Signature and Disclaimer, ce service peut être désactivé (voir Désactiver Signature and Disclaimer à la page 567).

Pour de plus amples informations sur la résolution d'erreurs courantes, voir Élimination des erreurs à la page 599.

Utilisation mobile de Signature and Disclaimer

Si Signature and Disclaimer est activé, les signatures et disclaimers sont également attachés aux courriels envoyés depuis des appareils mobiles.

REMARQUE :

Nous supportons la dernière version des systèmes d'exploitation Android et iOS. Pour les versions antérieures, il se peut que les signatures et les disclaimers ne s'affichent pas correctement.

Accès au module Signature and Disclaimer

Si des utilisateurs sans droits d'administrateur doivent être autorisés à créer et à modifier des signatures et des clauses de non-responsabilité, attribuez leur le rôle **Marketing** (voir « Rôles » dans le manuel du Control Panel). Le rôle **Marketing** donne aux utilisateurs l'accès au module **Signature and Disclaimer** (voir À propos de Signature and Disclaimer à la page 554).

Activer Signature and Disclaimer

Vous vous avez activé la synchronisation via LDAP (voir « Activer la connexion LDAP » dans le manuel du Control Panel) pour le domaine pour lequel vous souhaitez activer Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554).

Dans le module **Paramètres de sécurité** > **Signature and Disclaimer**, vous pouvez activer Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez activer Signature and Disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Cochez la case **Activer Signature and Disclaimer**.

Illustration 404 : Activer Signature and Disclaimer

Une fenêtre de confirmation apparaît.

5. Cliquez sur **Confirm**.

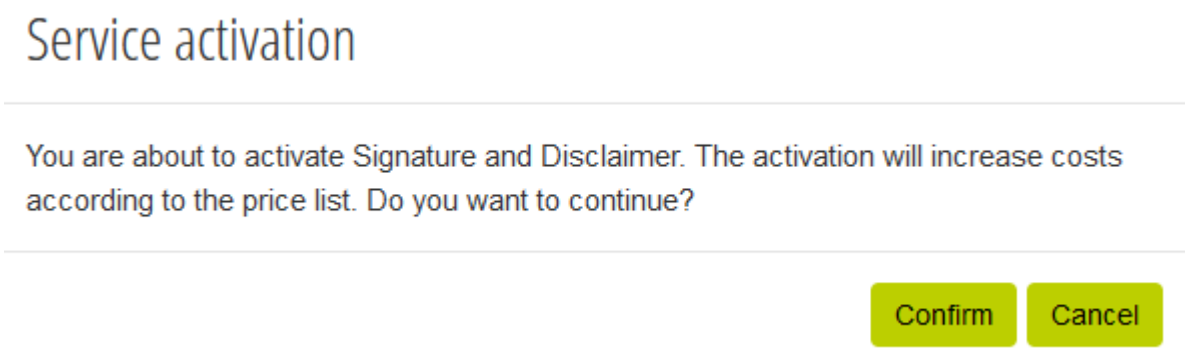


Illustration 405 : Confirmer l' activation

Signature and Disclaimer est activé.

Signature and Disclaimer a été activé.

Vous pouvez ensuite modifier les priorités des groupes (voir Modifier les priorités des groupes à la page 563). Vous pouvez également créer (voir Créer des signatures et des disclaimers à la page 558), traiter ou supprimer des signatures et des disclaimers (voir Éditer ou supprimer une signature ou un disclaimer à la page 565). Si vous ne souhaitez plus utiliser Signature and Disclaimer, vous pouvez désactiver le service (voir Désactiver Signature and Disclaimer à la page 567).

Créer des signatures et des disclaimers

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Dans le module **Paramètres de sécurité** > **Signature and Disclaimer**, vous pouvez créer des signatures ou disclaimers basés sur des groupes. Les groupes sont visibles sur le côté gauche de la fenêtre d'aperçu. Si vous n'avez créé aucun groupe pour le domaine, vous pouvez sélectionner le groupe **default** pour attribuer à tous les utilisateurs la même signature ou le même disclaimer.

REMARQUE :

Dans le Control Panel, vous pouvez créer sous **Paramètres client** > **Groupes** des nouveaux groupes. Vous trouverez de plus amples informations dans le manuel du Control Panel sous « Groupes ».

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer des signatures et des disclaimers.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.

4. Ajoutez sous **Groups** sur le côté gauche de la fenêtre d'aperçu un groupe issu de la sélection des groupes.

> **REMARQUE :**
>
> Si vous cliquez dans le champ **Search**, un menu déroulant apparaît ici avec tous les groupes créés. En outre, vous pouvez rechercher des groupes définis ici.

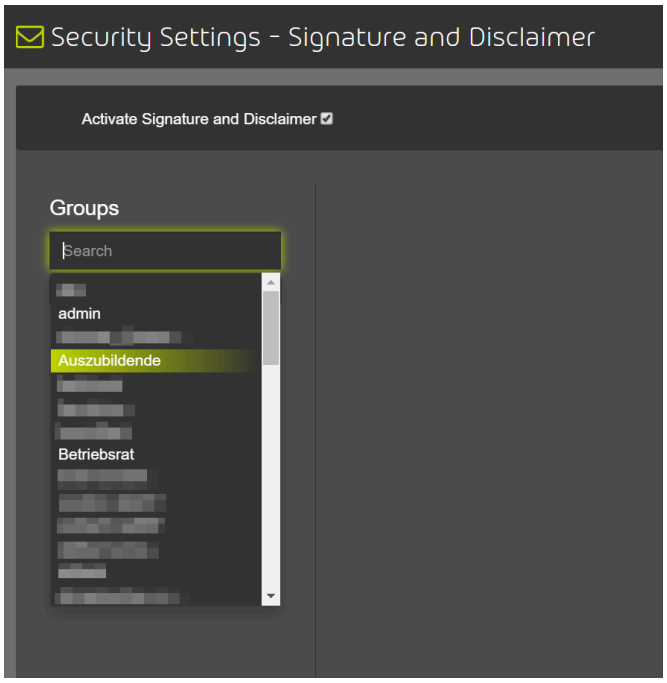


Illustration 406 : Ajouter un groupe

5. Sélectionnez le groupe ajouté.

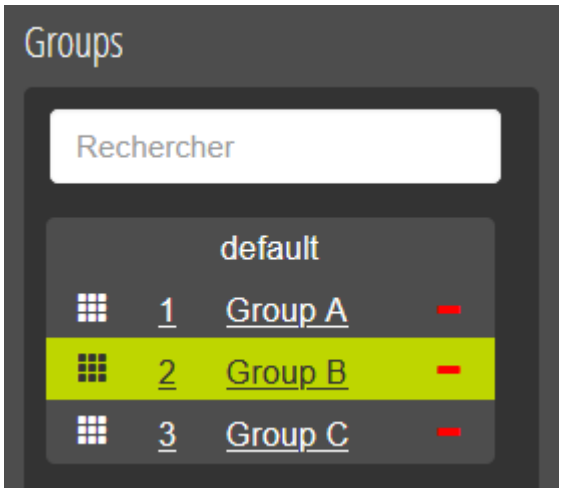


Illustration 407 : Sélectionner le groupe

Sur le côté droit de la fenêtre d'aperçu apparaît la sélection du disclaimer et de la signature.

6. Cliquez sur le côté droit sous **disclaimer** ou **Signature** sur **+** pour créer un nouveau modèle.

Illustration 408 : Ajouter un nouveau modèle

7. Saisissez un nom pour le nouveau modèle.

Vous pouvez créer un modèle de signatures ou de disclaimers à la fois au format HTML et Plain. Les modèles sont créés séparément.

8. Sélectionnez le format pour lequel vous souhaitez créer le modèle :
   - HTML
   - Plain

> **REMARQUE :**
>
> Vous pouvez passer d'un format à l'autre pendant l'édition.

9. Définissez votre modèle dans l'éditeur What You See Is What You Get (éditeur WYSIWYG) (voir Éditeur WYSIWYG à la page 568).

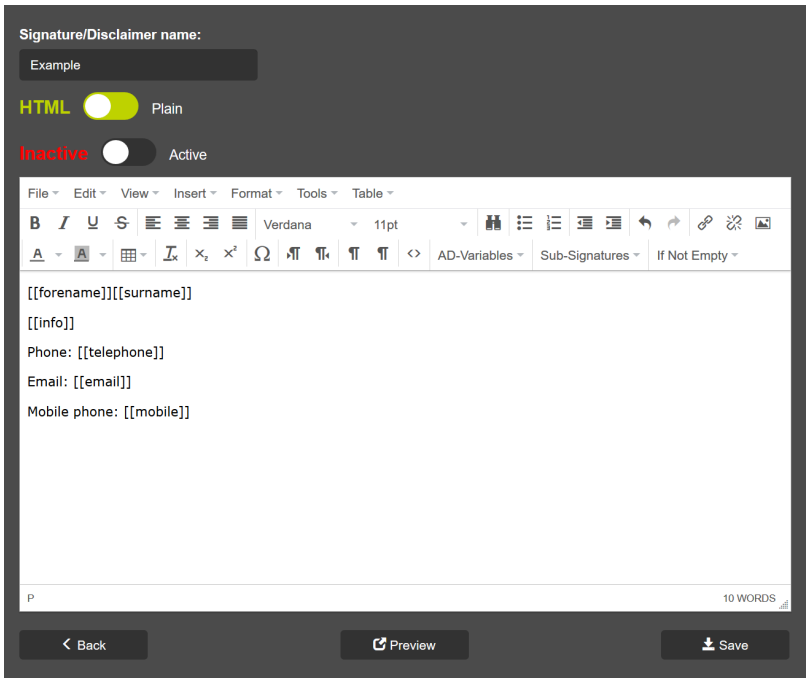


Illustration 409 : Créer un modèle dans l' éditeur WYSIWYG

10. Enregistrez le modèle.

11. Sélectionnez le modèle dans la fenêtre d'aperçu.

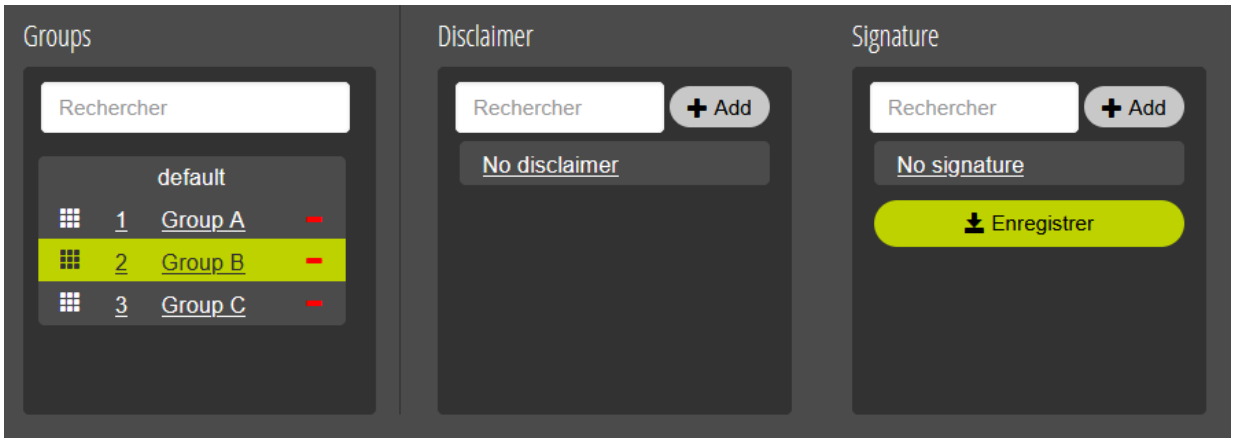


Illustration 410 : Sélection de la signature dans la fenêtre d' aperçu

12. Cliquez dans l'aperçu sur **Enregistrer** pour attribuer le modèle sélectionné auparavant dans le groupe sélectionné.

Vous avez créé une signature et/ou un disclaimer et l'avez attribué(e) à un groupe.

REMARQUE :

Les signatures et disclaimers sont uniquement ajoutés aux courriels qui sont envoyés via les adresses de serveurs de relais saisies dans **Spam and Malware Protection** (voir «#Configuration d'environnement principal#» dans le manuel du Control Panel).

REMARQUE :

La signature et la clause de non-responsabilité d'un utilisateur ne sont jointes qu'une seule fois dans une discussion courriel. La répétition des signatures et des clauses de non responsabilité dans la suite de la discussion courriel est évitée dans la mesure du possible.

Modifier les priorités des groupes

Vous avez ajouté plusieurs groupes au module **Signature and Disclaimer** (voir Créer des signatures et des disclaimers à la page 558).

Dans le module **Signature and Disclaimer**, les groupes sont classés en fonction de leur priorité. Les priorités des groupes sont affichées dans le tableau des groupes sous **Groupes**. Plus le nombre est bas, plus un groupe est prioritaire. Si une boîte aux lettres appartient à plusieurs groupes dans le module **Signature and Disclaimer**, les courriels sortants de la boîte aux lettres sont envoyés avec la signature et le disclaimer du groupe avec la priorité la plus élevée.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour les groupes duquel vous souhaitez modifier les priorités dans le module **Signature and Disclaimer**.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Sous **Groupes**, sélectionnez le groupe dont vous souhaitez modifier la priorité.

5. Facultatif : Modifiez la priorité du groupe en déplaçant le groupe dans la liste.

   a) Cliquez sur le symbole à neuf points à côté du groupe et maintenez le bouton gauche de la souris enfoncé.

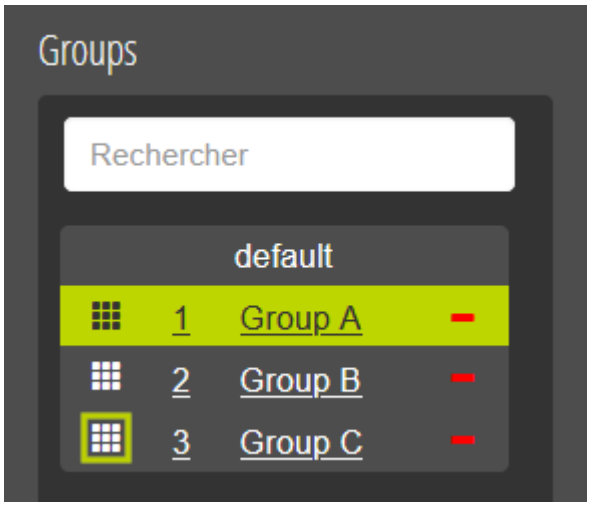


Illustration 411 : Déplacer un groupe

   b) Faites glisser le groupe vers la position qui correspond à la nouvelle priorité.

   c) Relâchez le bouton gauche de la souris.

Le groupe est placé à la nouvelle position. Les priorités de tous les groupes qui se sont déplacés dans la liste sont actualisées.

6. Écrasez la priorité du groupe.

   a) Double-cliquez sur la priorité à côté du groupe.

Le nombre peut maintenant être modifié.

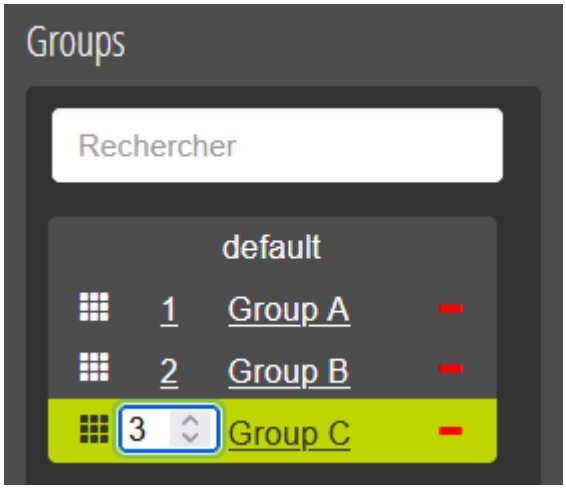


Illustration 412 : Champ de saisie pour la priorité

b) Saisissez le nombre de la nouvelle priorité dans le champ de saisie ou sélectionnez le nombre à l'aide des flèches de sélection.

c) Confirmez la nouvelle priorité à l'aide de la touche Entrée.

La priorité du groupe est enregistrée. Le groupe est placé à la position qui correspondant à la nouvelle priorité. Les priorités de tous les groupes qui se sont déplacés dans la liste sont actualisées.

Les priorités des groupes ont été modifiées.

Éditer ou supprimer une signature ou un disclaimer

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556) et créé une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558).

Le module **Paramètres de sécurité** > **Signature and Disclaimer** vous permet d'éditer ou de supprimer des signatures ou des disclaimers existants.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez éditer ou supprimer une signature ou un disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Dans la fenêtre d'aperçu, cliquez dans le champ **Rechercher** sous **Disclaimer** ou **Signature** et sélectionnez le modèle désiré.

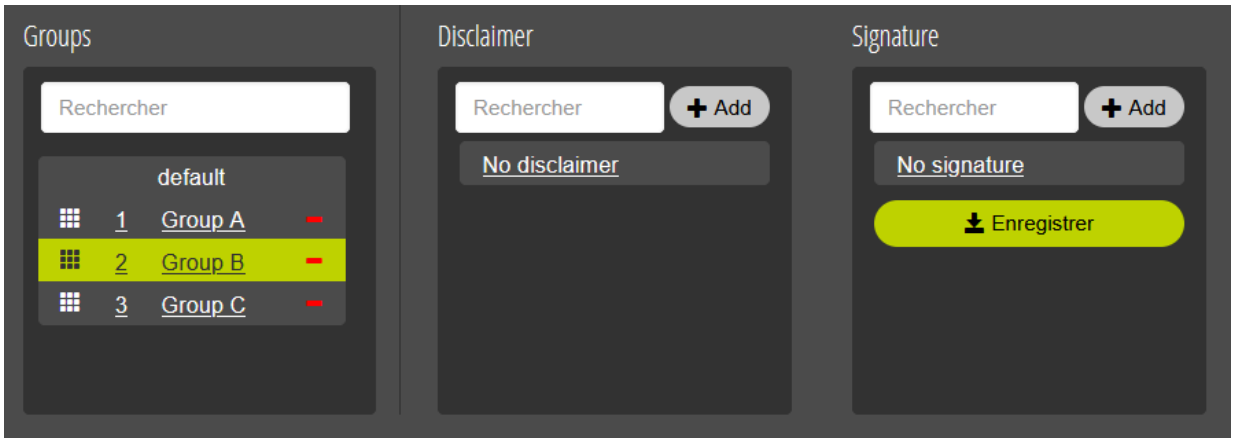


Illustration 413 : Sélection de la signature dans la fenêtre d' aperçu

5. Sélectionnez l'une des actions suivantes :

   - Pour éditer le modèle sélectionné, cliquez sur le symbole du stylo derrière le nom du modèle. L'éditeur apparaît et vous pouvez éditer le modèle.

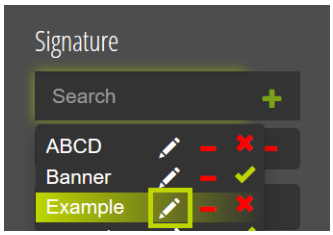


Illustration 414 : Éditer le modèle

   - Pour supprimer le modèle sélectionné, cliquez sur le **-** rouge. Confirmez la saisie avec **OK**.

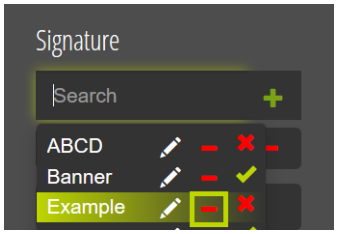


Illustration 415 : Supprimer le modèle

Une signature ou un disclaimer a été édité ou supprimé.

Désactiver Signature and Disclaimer

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Si vous ne souhaitez plus utiliser Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554), vous pouvez désactiver ce service. Vos paramètres de groupe, vos signatures et vos clauses de non-responsabilité restent conservées au cas où vous voudriez réactiver Signature and Disclaimer ultérieurement.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez désactiver Signature and Disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Décochez la case **Activer Signature and Disclaimer**.

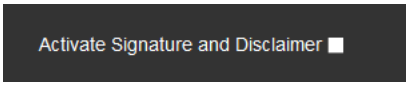


Illustration 416 : Désactiver Signature and Disclaimer

Une fenêtre de confirmation s'ouvre.

5. Cliquez sur **OK**.

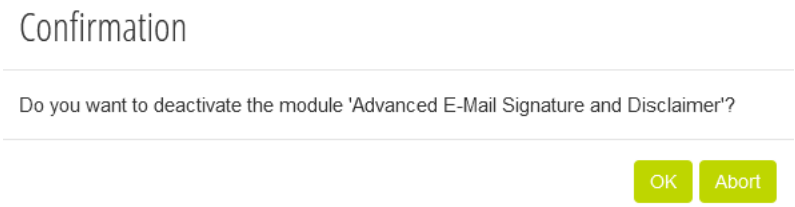


Illustration 417 : Confirmer la désactivation

Signature and Disclaimer est désactivé.

Signature and Disclaimer a été désactivé.

> **REMARQUE :**
>
> La désactivation de Signature and Disclaimer n'entraîne pas la résiliation du contrat existant pour ce service. Pour annuler un contrat existant, vous devez contacter votre interlocuteur.

Éditeur WYSIWYG

Dans l'éditeur WYSIWYG, des modèles de disclaimers et de signatures peuvent facilement être créés et édités.

Pour ce faire, les administrateurs et les utilisateurs avec le rôle **Marketing** (voir Accès au module Signature and Disclaimer à la page 556) peuvent utiliser des options de formatage simples telles que la modification de l'alignement des paragraphes ou de la police de caractères. Par ailleurs, il est possible d'accéder, via les variables Active Directory, aux attributs depuis Active Directory ou aux données de base des boîtes aux lettres créées manuellement (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel) pour ajouter par exemple les noms et prénoms définis dans la boîte aux lettres correspondante dans les signatures ou disclaimers. Les attributs disponibles dépendent de l'application :

- Lorsque la connexion LDAP (voir « Connexion LDAP » dans le manuel du Control Panel) est activée, de nombreux attributs sont disponibles depuis Active Directory (voir Attributs synchronisés depuis Active Directory à la page 570). Si aucune valeur n'est attribuée à un attribut, celui-ci peut être masqué dans les signatures et les disclaimer (voirNe pas afficher les éléments Active Directory vides à la page 576).
- Pour les boîtes aux lettres créées manuellement, les données de base des boîtes aux lettres (voir Demande de données de base avec variables AD à la page 574) sont disponibles.

> **IMPORTANT :**
>
> La condition pour l'utilisation de variables AD est qu'elles aient été définies dans Active Directory.

Les signatures et les disclaimers peuvent être formatés à l'aide du texte source HTML (voir Ajouter un texte source HTML à la page 582). En outre, les signatures existantes peuvent être intégrées dans d'autres signatures en tant que sous-signatures (voir Intégrer des sous-signatures à la page 579) et des graphiques peuvent être ajoutés aux signatures et aux disclaimers (voir Intégration des graphiques dans les signatures et disclaimers à la page 584). Une fonction de prévisualisation permet de voir comment une signature ou un disclaimer sera émis par la suite (voir Afficher une prévisualisation d' une signature ou d' un disclaimer à la page 583).

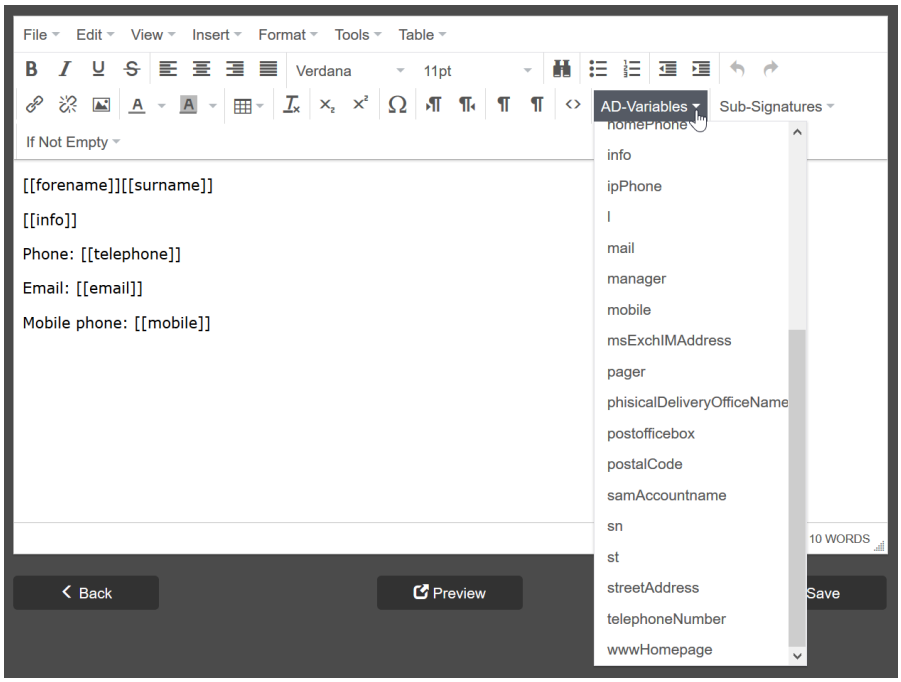


Illustration 418 : Éditeur WYSIWYG

Attributs synchronisés depuis Active Directory

Si la connexion LDAP (voir « Connexion LDAP » dans le manuel du Control Panel) est activée, de nombreux attributs sont synchronisés avec l'Active Directory de Microsoft et peuvent être utilisés dans le module **Signature and Disclaimer** (voir À propos de Signature and Disclaimer à la page 554). Dès que des données sont modifiées dans l'Active Directory, celles-ci seront également actualisées dans le Control Panel (voir Synchronisation des données via LDAP à la page 572).

Les attributs suivants d'Active Directory sont synchronisés pour les boîtes aux lettres LDAP (voir le chapitre « Types de boîtes aux lettres » dans le manuel du Control Panel) et peuvent être utilisés pour la création de signatures et de disclaimers :

VARIABLE AD	SIGNIFICATION
cn	« Common Name » – nom d'usage

VARIABLE AD	SIGNIFICATION
company	Entreprise
countryCode	Pays/région
department	Département
description	Description
directReports	Collaborateurs
displayName	Nom affiché – Nom complet
facsimileTelephoneNumber	Fax
givenName	Prénom
homePhone	Numéro de téléphone privé
info	Titre du job/poste
ipPhone	Numéro de téléphone IP
l (L minuscule)	Ville
mail	définir une adresse e-mail
manager	Supérieur(e)

REMARQUE :

Le champ Title est souvent utilisé différemment. Par conséquent, l'attribut LDAP Title (titre de job/poste) est appelé Info.

VARIABLE AD	SIGNIFICATION
mobile	Numéro de téléphone portable
msExchIMAddress	Adresse IM
pager	N° de téléavertisseur
physicalDeliveryOfficeName	Bureau
postalCode	Code postal
postOfficeBox	boîte aux lettres
samAccountName	Nom de connexion de l'utilisateur
sn	Nom
st	État fédéral/Canton
streetAddress	Rue
telephoneNumber	Numéro de téléphone
wwwHomepage	site Web

Synchronisation des données via LDAP

Si vous apportez des modifications à Active Directory, ces modifications sont synchronisées.

Les modifications apportées à Active Directory sont suivies à l'aide de l'attribut **USNChangedNr**. Si la valeur change, l'ensemble de données est synchronisé.

IMPORTANT :

Si vous importez une sauvegarde, le **USNChangedNr** n'est pas augmenté, mais réinitialisé à un état antérieur. L'ensemble de données est ensuite de nouveau synchronisé.

Attributs synchronisés de l' Azure Active Directory

Avec Azure Active Directory de Microsoft, certains attributs pour Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554) sont synchronisés.

IMPORTANT :

Pour les boîtes aux lettres créées manuellement, les données de base (voir Demande de données de base avec variables AD à la page 574) sont utilisées. Les attributs LDAP ne sont pas synchronisés et ne peuvent pas être utilisés.

Les attributs suivants sont synchronisés et peuvent être utilisés pour créer des signatures et des disclaimers :

VARIABLE AD	SIGNIFICATION
countryCode	Pays/région
department	Département
displayName	Nom affiché – Nom complet
givenName	Prénom

VARIABLE AD	SIGNIFICATION
info	Titre du job/poste **REMARQUE :** Le champ title est souvent utilisé différemment. Par conséquent, l'attribut LDAP Title (titre de job/poste) est appelé Info.
l (L minuscule)	Ville
mail	Adresse courriel
mobile	Numéro de téléphone portable
postalCode	Code postal
sn	Nom
st	État fédéral/Canton
streetAddress	Rue
telephoneNumber	Numéro de téléphone

Demande de données de base avec variables AD

IMPORTANT :

Pour les boîtes aux lettres créées manuellement, il est possible d'utiliser les données de base des boîtes aux lettres décrites ici comme variables AD.

Les correspondances suivantes existent entre les variables AD et les données de base d'une boîte aux lettres :

VARIABLE AD	DATE DE BASE
countryCode	**Pays/région**
department	**Département**
displayName	**Nom affiché**
facsimileTelephoneNumber	**Fax**
givenName	**Prénom**
l (L minuscule)	**Localité**
mail	Adresse courriel de la boîte aux lettres
mobile	**Téléphone mobile**
postalCode	**Code postal**
phisicalDeliveryOfficeName	**Bureau**
sn	**Nom**
st	**État**
streetAddress	**Rue, numéro**
telephoneNumber	**Téléphone (professionnel)**

Ne pas afficher les éléments Active Directory vides

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Dans le module **Paramètres de sécurité** > **Signature and Disclaimer**, la fonction **If Not Empty** de l'éditeur WYSIWYG (voir Éditeur WYSIWYG à la page 568) vous permet de masquer du contenu dans les signatures et les disclaimers dans le cas où certaines variables AD ne seraient pas remplies pour des utilisateur.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer des signatures et des disclaimers.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Créez ou traitez une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Dans l'éditeur, sélectionnez la ligne dans laquelle la variable AD doit être incluse.
6. Cliquez sur **If Not Empty**.

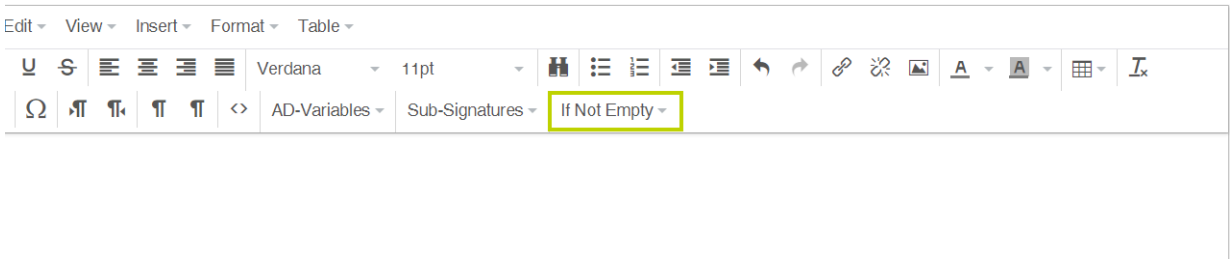


Illustration 419 : Ouvrir la sélection

7. Sélectionnez la variable AD désirée dans le champ Variable.

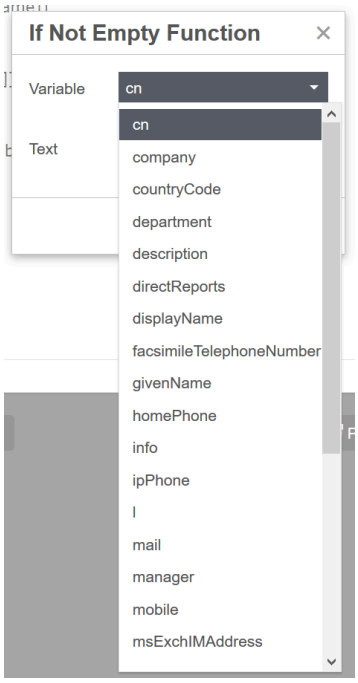


Illustration 420 : Sélectionner une variable AD

8. Saisissez le texte à masquer si l'élément n'est pas rempli pour l'utilisateur.
9. Confirmez avec **OK**.

10. Il est également possible de saisir une variable AD dans le texte à masquer :

a) Cliquez sur la position dans l'éditeur entre la balise If Not Empty où vous voulez insérer la variable AD à masquer.

b) Sélectionnez la variable AD dans le menu déroulant.

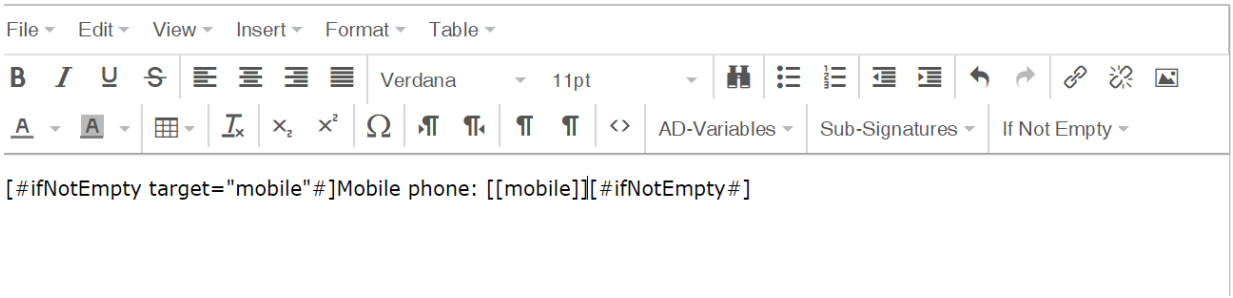


Illustration 421 : If Not Empty - Numéro de téléphone portable

11. Cliquez sur **Enregistrer** pour enregistrer la signature ou le disclaimer.

Des éléments vides de l'Active Directory ont été masqués d'une signature ou d'un disclaimer.

Exemple : cacher les variables non présentes

La signature suivante est utilisée pour tous les utilisateurs :

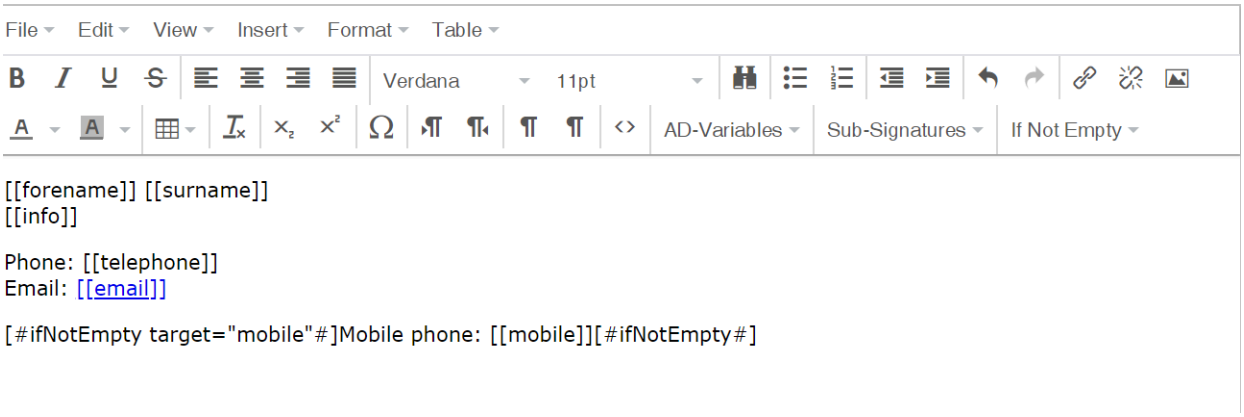


Illustration 422 : Signature dans l' éditeur

La signature suivante est utilisée pour les utilisateurs avec numéro de téléphone portable :

John Doe
Chief Executive Officer

Phone: +49 123456 789
Email: jdoe@domain.tld

Mobile phone: +49 123456 789

Illustration 423 : Signature avec numéro de téléphone portable

La signature suivante est utilisée pour les utilisateurs sans numéro de téléphone portable :

Jane Doe
Product Management

Phone: +49 123456 789
Email: jadoe@domain.tld

Illustration 424 : Signature sans numéro de téléphone portable

Intégrer des sous-signatures

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556). Vous avez créé une signature (voir Créer des signatures et des disclaimers à la page 558).

Dans le module **Paramètres de sécurité** > **Signature and Disclaimer**, la fonction **Sub-Signatures** de l'éditeur WYSIWYG (voir Éditeur WYSIWYG à la page 568) permet d'inclure une signature existante en tant que sous-signature dans une autre signature de Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554).

IMPORTANT :

Les sous-signatures ne peuvent être utilisées que pour les signatures. Il doit également y avoir au moins une signature que vous pouvez inclure comme sous-signature.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une signature.

3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Créez ou éditez une signature (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Dans l'éditeur, sélectionnez la ligne de la signature dans laquelle la sous-signature doit être incluse.
6. Cliquez sur **Sub-Signatures** et sélectionnez la sous-signature requise parmi les signatures existantes.

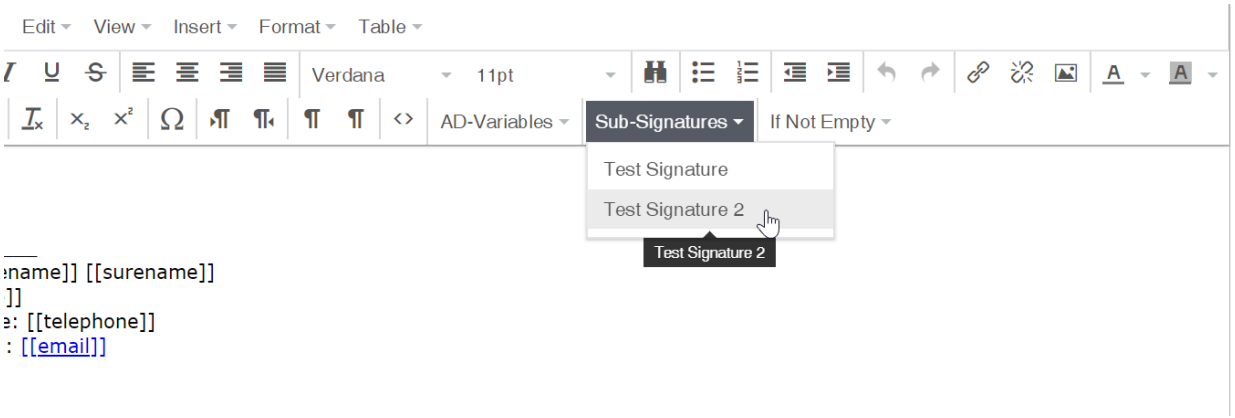


Illustration 425 : Sélectionner une sous-signature

Un caractère de remplacement est inséré pour la sous-signature.

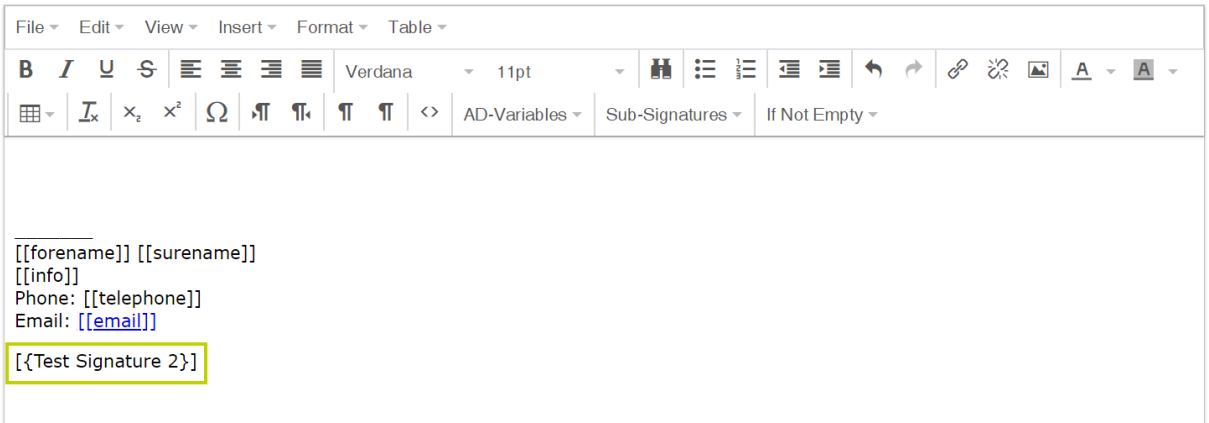


Illustration 426 : Sous-signature Caractère de remplacement

7. Cliquez sur **Enregistrer** pour enregistrer la signature avec sous-signature.
8. **IMPORTANT :**

   Pour qu'une signature puisse être utilisée comme sous-signature, la signature doit être activée pour celle-ci.

   Pour activer une signature à utiliser comme sous-signature :

   a) Ouvrez le mode d'édition de la signature que vous voulez utiliser comme sous-signature.

   b) Mettez l'interrupteur sur **Cryptage actif**.

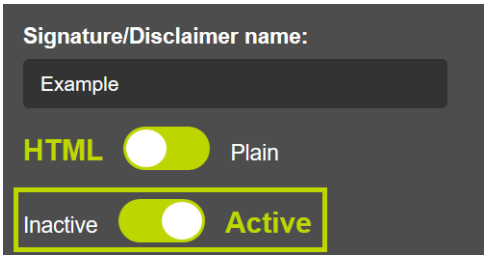


Illustration 427 : Activer les sous-signatures

Les signatures activées et désactivées sont marquées dans la sélection de signature.

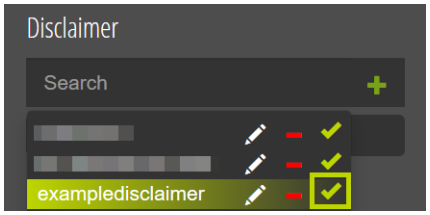


Illustration 428 : Signature activée dans la sélection

Illustration 429 : Signature désactivée dans la sélection

Une sous-signature a été intégrée dans une signature.

Ajouter un texte source HTML

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Dans le module **Paramètres de sécurité** > **Signature and Disclaimer**, vous pouvez ajouter du code source HTML aux signatures et aux disclaimers à l'aide de l'éditeur WYSIWYG.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une signature ou un disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Créez ou traitez une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Dans l'éditeur WYSIWYG, cliquez sur la rubrique **Tools** et sélectionnez le point **Source Code**.

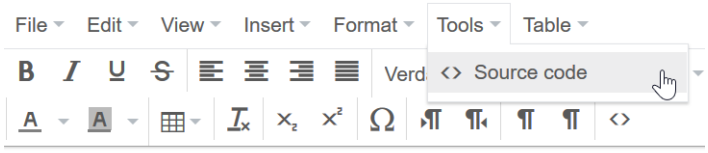


Illustration 430 : Éditeur de texte source

Une nouvelle fenêtre de saisie de texte apparaît.

6. Ajoutez le texte source HTML désiré et confirmez avec **OK**.

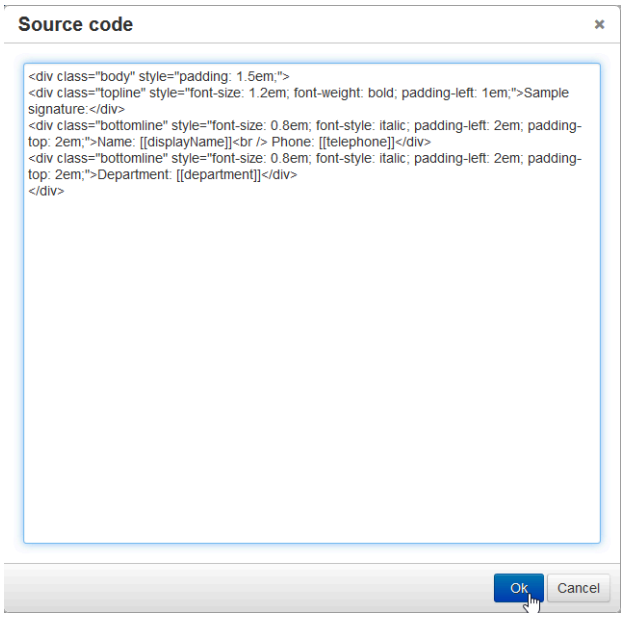


Illustration 431 : Ajouter le texte source

7. Enregistrez ensuite votre modèle et cliquez sur **Enregistrer**.

Le texte source HTML a été ajouté à une signature ou à un disclaimer.

Afficher une prévisualisation d'une signature ou d'un disclaimer

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Le module **Paramètres de sécurité** > **Signature and Disclaimer** vous permet d'afficher une prévisualisation d'une signature ou d'un disclaimer.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une signature ou un disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.

4. Créez ou modifiez une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Dans l'éditeur WYSIWYG, en-dessous, cliquez sur **Prévisualisation**.

Une fenêtre de prévisualisation des signatures et des disclaimers s'ouvre.

6. Sélectionnez une boîte aux lettres dans la liste à gauche de la fenêtre.

Une prévisualisation de la signature et/ou du disclaimer de l'utilisateur sélectionné s'affiche à droite dans la fenêtre.

Une prévisualisation d'une signature et/ou d'un disclaimer a été affiché.

Intégration des graphiques dans les signatures et disclaimers

L'éditeur WYSIWYG vous permet d'ajouter des graphiques aux signatures et disclaimers. Les graphiques qui doivent être utilisés pour toutes les boîtes aux lettres d'un groupe peuvent être soit copiés directement dans l'éditeur WYSIWYG par glisser-déposer (voir Insérer et mettre des graphiques en hyperlien par glisser-déposer à la page 589), soit intégrés comme URL via une fenêtre de saisie (voir Intégrer un graphique à l'aide d'une URL à la page 584). En outre, il est possible d'intégrer différents graphiques dans les signatures et les disclaimers pour les différentes boîtes aux lettres d'un groupe (voir Intégrer différents graphiques pour des boîtes aux lettres différentes à la page 592).

Intégrer un graphique à l'aide d'une URL

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556).

Le module **Paramètres de sécurité** > **Signature and Disclaimer** vous permet d'intégrer un graphique dans une signature ou un disclaimer via une URL. Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.

2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une signature ou un disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Créez ou éditez une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Lors de la création ou la modification de la signature ou du disclaimer dans l'éditeur WYSIWYG, cliquez à l'endroit où vous souhaitez insérer le graphique.
6. Naviguez dans la barre de menu de l'éditeur vers **Insert** > **Image**.

Une fenêtre de saisie avec d'autres paramètres s'ouvre.

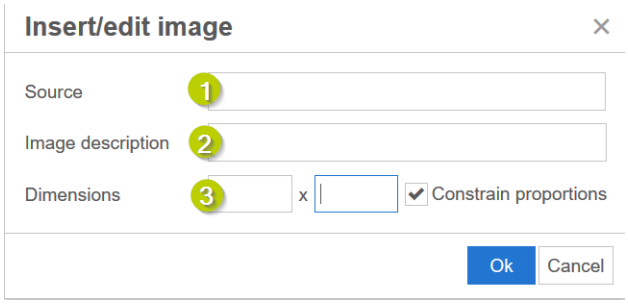


Illustration 432 : Fenêtre de saisie pour les graphiques

7. Saisissez sous **Source** (1) l'adresse du graphique qui doit être affiché et qui est représentatif de votre lien. Recherchez sur Internet le graphique souhaité et copiez l'adresse graphique enregistrée.

Illustration 433 : Copier l' adresse du graphique représentatif et ajouter sous Source

L'adresse du graphique souhaité est enregistrée.

8. Saisissez sous **Image description** (2) alternativement une description.
9. Adaptez sous **Dimensions** (3) la taille du graphique individuellement et enregistrez vos saisies avec **Ok**.

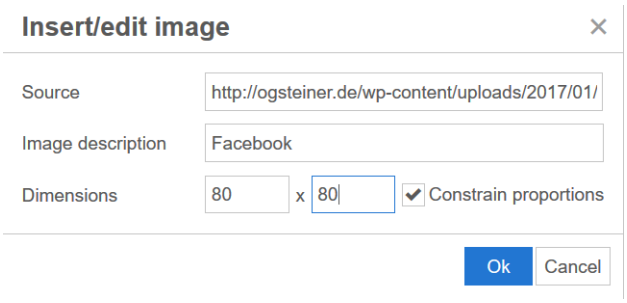


Illustration 434 : Modifier la taille du graphique

Les paramètres ont été enregistrés et le graphique est affiché dans l'éditeur.

10. Cliquez avec le bouton droit de la souris sur le graphique ajouté et sélectionnez **Lien** pour saisir un URL vers lequel il doit renvoyer.

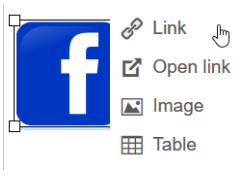


Illustration 435 : Mettre le graphique en hyperlien

Une fenêtre de saisie avec d'autres paramètres s'ouvre.

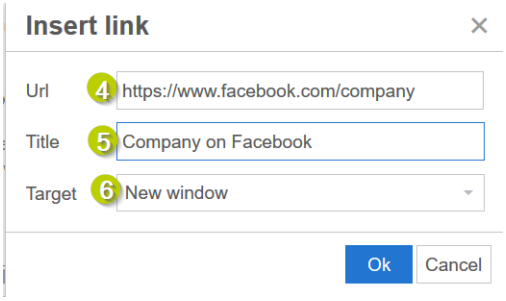


Illustration 436 : Saisir l' URL

11. Sous **URL** (4), saisissez l'adresse cible du site Web désiré.
12. Sous **Title** (5), saisissez alternativement un texte qui doit être affiché lorsque l'on passe la souris sur le graphique.
13. Sélectionnez sous **Target** (6) l'option **New window** pour ouvrir le site Web du lien dans un nouvel onglet.
14. Cliquez sur **Ok** puis sur **Enregistrer** pour enregistrer toutes les informations.

> **REMARQUE :**
>
> Si nécessaire, répétez les étapes 1 à 10 si vous souhaitez insérer plusieurs graphiques.

Un graphique a été intégré dans une signature ou un disclaimer via une URL.

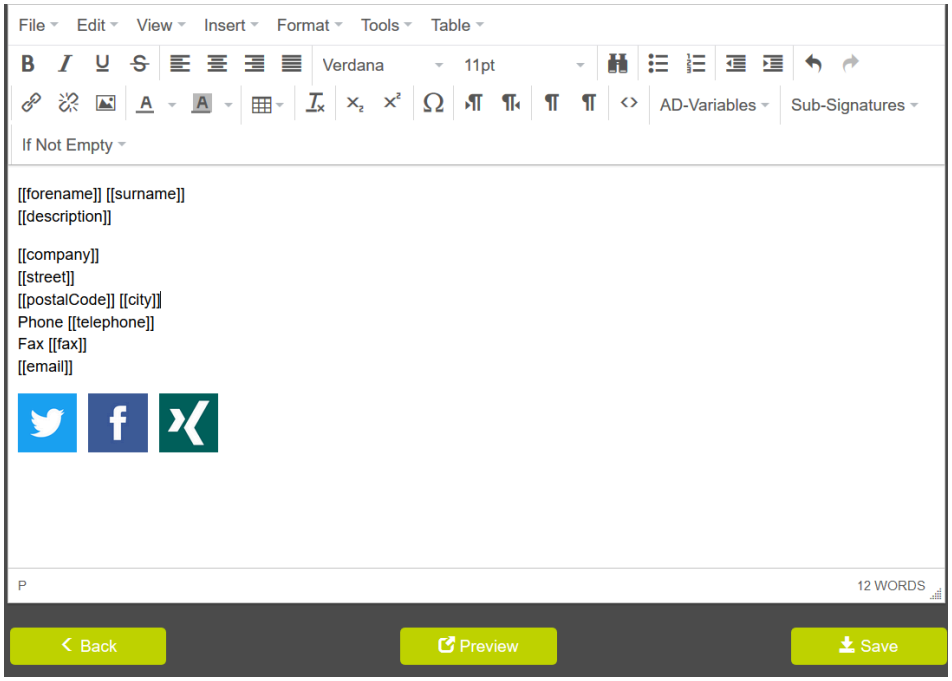


Illustration 437 : Affectation de variables avec graphiques mis en hyperlien

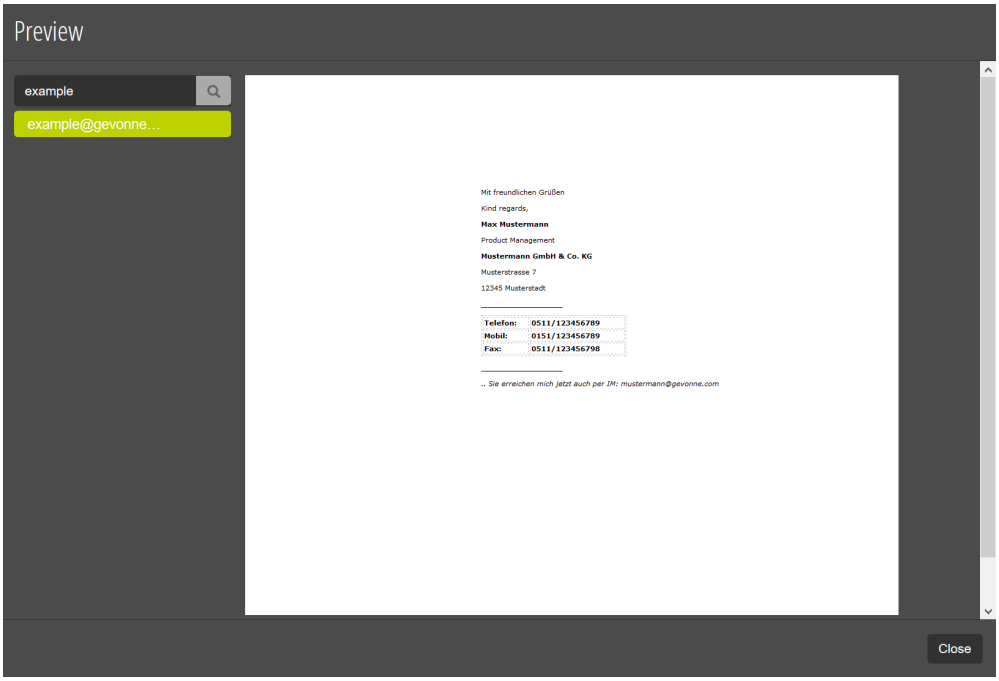


Illustration 438 : Aperçu de la signature créée avec les graphiques mis en hyperlien

Insérer et mettre des graphiques en hyperlien par glisser-déposer

Le module **Paramètres de sécurité** > **Signature and Disclaimer** vous permet d'insérer un graphique par glisser-déposer dans une signature ou un disclaimer de Signature and Disclaimer (voir À propos de Signature and Disclaimer à la page 554) et de créer un lien vers ce graphique.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez créer une signature ou un disclaimer.
3. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
4. Créez ou modifiez une signature ou un disclaimer (voir Créer des signatures et des disclaimers à la page 558 ou Éditer ou supprimer une signature ou un disclaimer à la page 565).
5. Lors de la création ou la modification de la signature ou du disclaimer dans l'éditeur WYSIWYG, cliquez à l'endroit où vous souhaitez insérer le graphique.

6. Faites glisser le graphique dans l'éditeur jusqu'à la position souhaitée.

Le graphique est inséré à la position souhaitée par glisser-déposer.

7. Cliquez avec le bouton droit de la souris sur le graphique ajouté et sélectionnez **Lien** pour saisir un URL vers lequel il doit renvoyer.

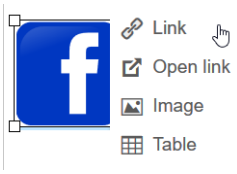


Illustration 439 : Mettre le graphique en hyperlien

Une fenêtre de saisie avec d'autres paramètres s'ouvre.

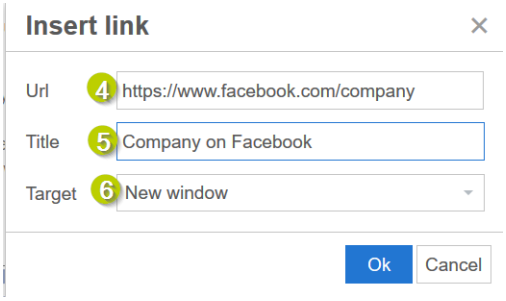


Illustration 440 : Saisir l' URL

8. Sous **URL** (4), saisissez l'adresse cible du site Web désiré.
9. Sous **Title** (5), saisissez alternativement un texte qui doit être affiché lorsque l'on passe la souris sur le graphique.
10. Sélectionnez sous **Target** (6) l'option **New window** pour ouvrir le site Web du lien dans un nouvel onglet.
11. Cliquez sur **Ok** et fermez la fenêtre de saisie.

Le graphique est mis en hyperlien.

12. Facultatif : Cliquez avec le bouton droit de la souris sur le graphique enregistré et sélectionnez **Image** pour ajuster la taille du graphique au champ **Dimensions**.

13. Cliquez sur **Ok** puis sur **Enregistrer** pour enregistrer toutes les informations.

> **REMARQUE :**
>
> Si nécessaire, répétez les étapes 1 à 9 si vous souhaitez insérer plusieurs graphiques.

Un graphique a été ajouté à une signature ou à un disclaimer par glisser-déposer.

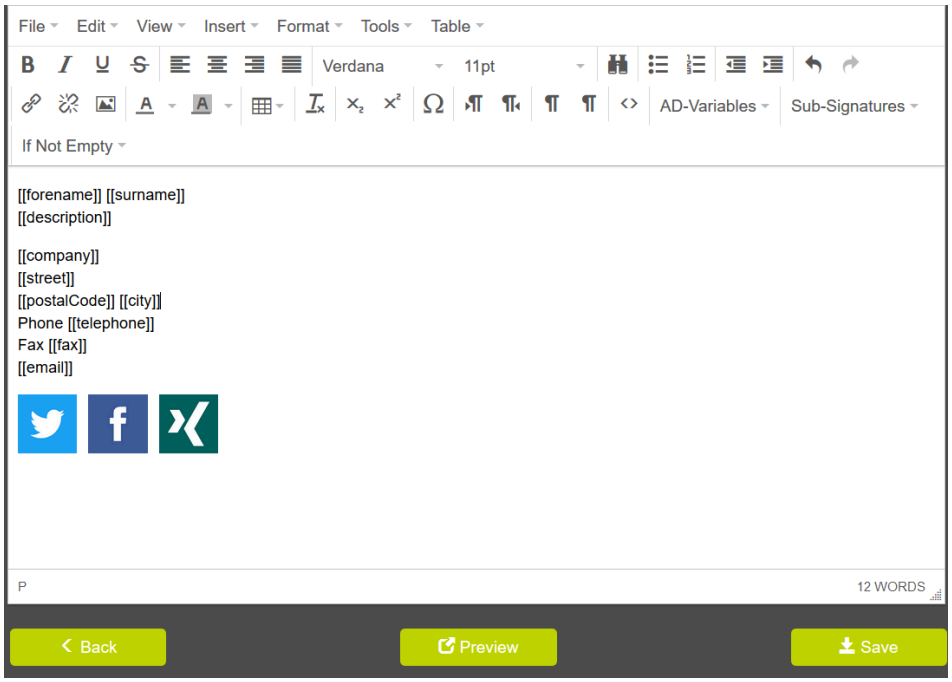


Illustration 441 : Affectation de variables avec graphiques mis en hyperlien

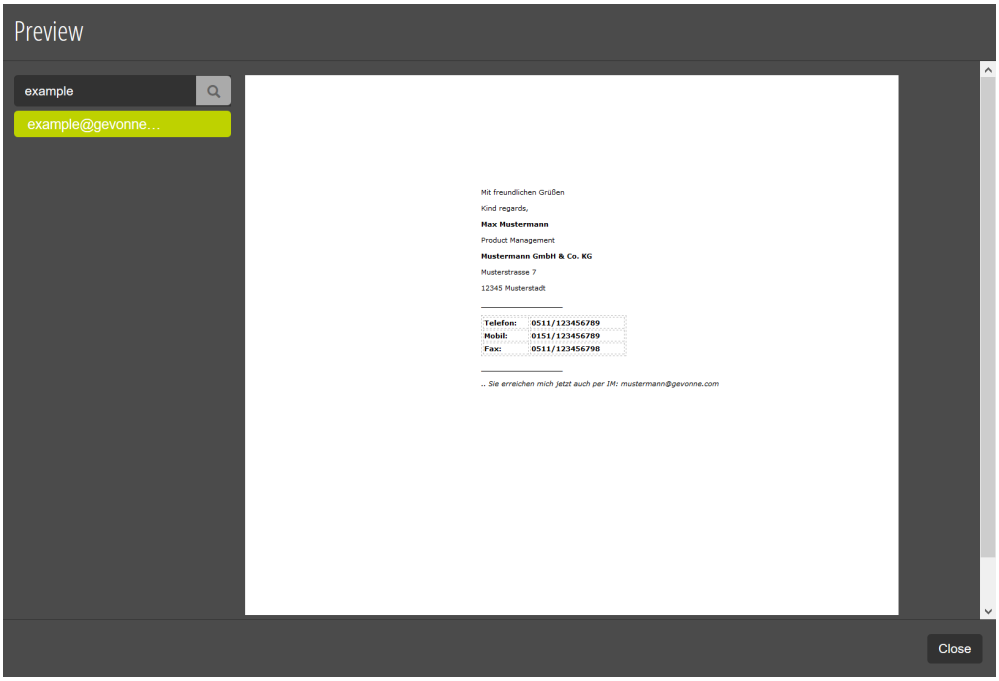


Illustration 442 : Aperçu de la signature créée avec les graphiques mis en hyperlien

Intégrer différents graphiques pour des boîtes aux lettres différentes

Vous avez activé Signature and Disclaimer (voir Activer Signature and Disclaimer à la page 556). Vous avez créé une boîte aux lettres (voir « Ajouter une boîte aux lettres » dans le manuel du Control Panel) et l'avez ajoutée à un groupe (voir « Ajouter une boîte aux lettres à un groupe » dans le manuel du Control Panel).

Les modules **Paramètres client** > **Boîtes aux lettres** et **Paramètres de sécurité** > **Signature and Disclaimer** (voir À propos de Signature and Disclaimer à la page 554) permettent d'intégrer différents graphiques dans les signatures des différentes boîtes aux lettres d'un groupe.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine souhaité dans la sélection de l'espace.
3. Naviguez vers **Paramètres client** > **Boîtes aux lettres**.

4. Cliquez sur la flèche de menu de la boîte aux lettres désirée.

Illustration 443 : Ouvrir le menu

Un menu s'ouvre.

5. Cliquez sur **Données de base**.

Un menu déroulant s'ouvre.

6. Saisissez l'adresse graphique d'une image dans un champ vide du **Données de base**.

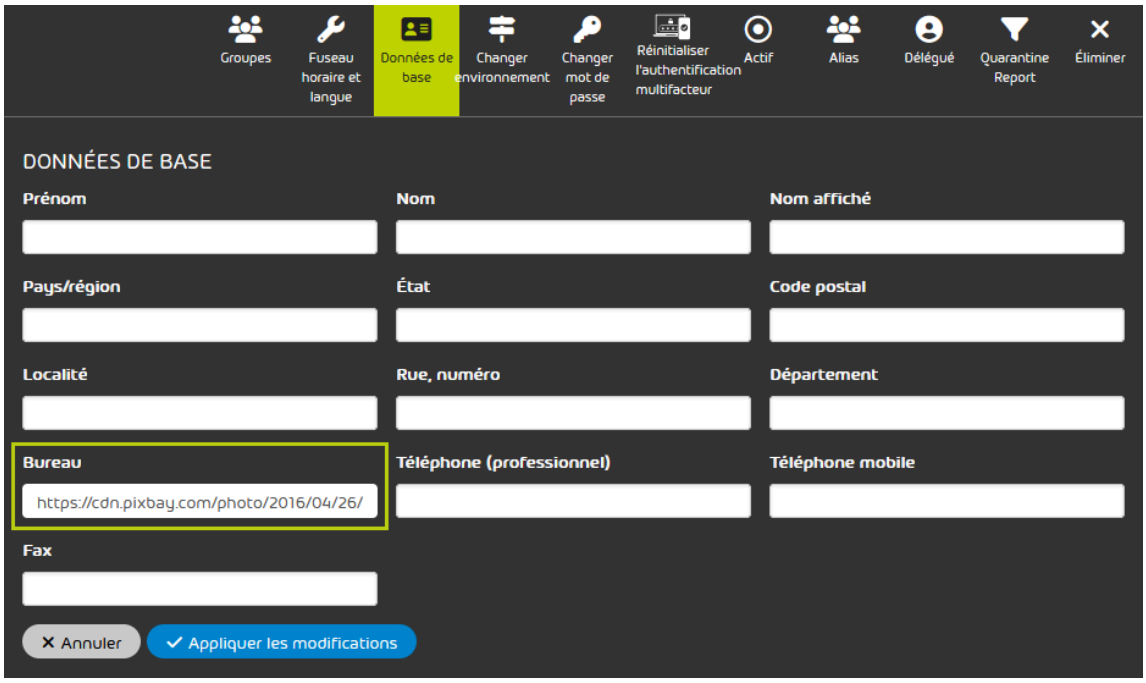


Illustration 444 : Saisir l'adresse graphique dans Bureau à titre d'exemple

7. Cliquez sur **Appliquer les modifications**.

Les modifications sont enregistrées.

8. Répétez la procédure pour chaque boîte aux lettres du groupe.
9. Naviguez vers **Paramètres de sécurité** > **Signature and Disclaimer**.
10. Sélectionnez le groupe où se trouve la boîte aux lettres éditée auparavant.

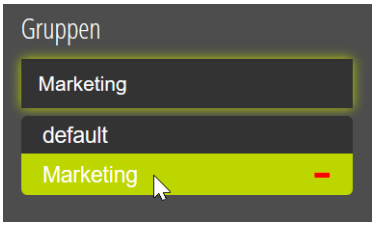
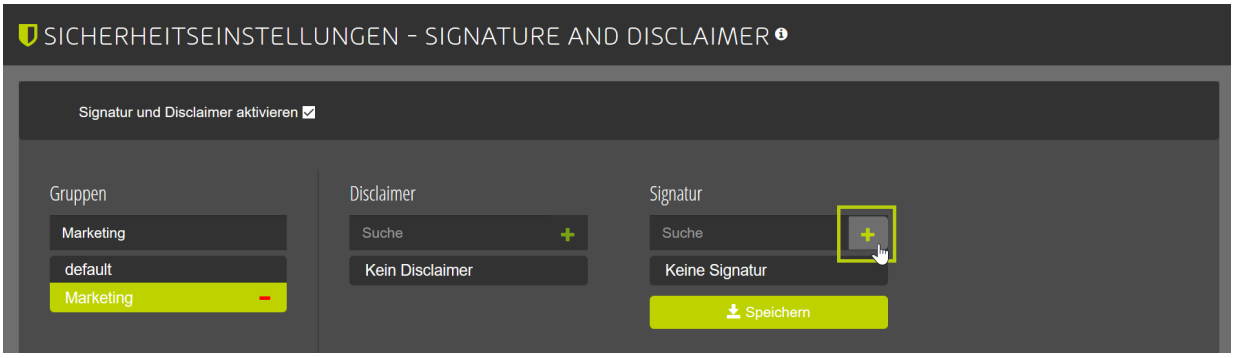


Illustration 445 : Sélectionner un groupe

Le groupe est sélectionné.

11. Cliquez sur le bouton avec le symbole plus sous l'entête **Signature**.



La fenêtre **Signature** s'ouvre.

12. Cliquez sur le bouton **Source code** dans la fenêtre **Signature**.

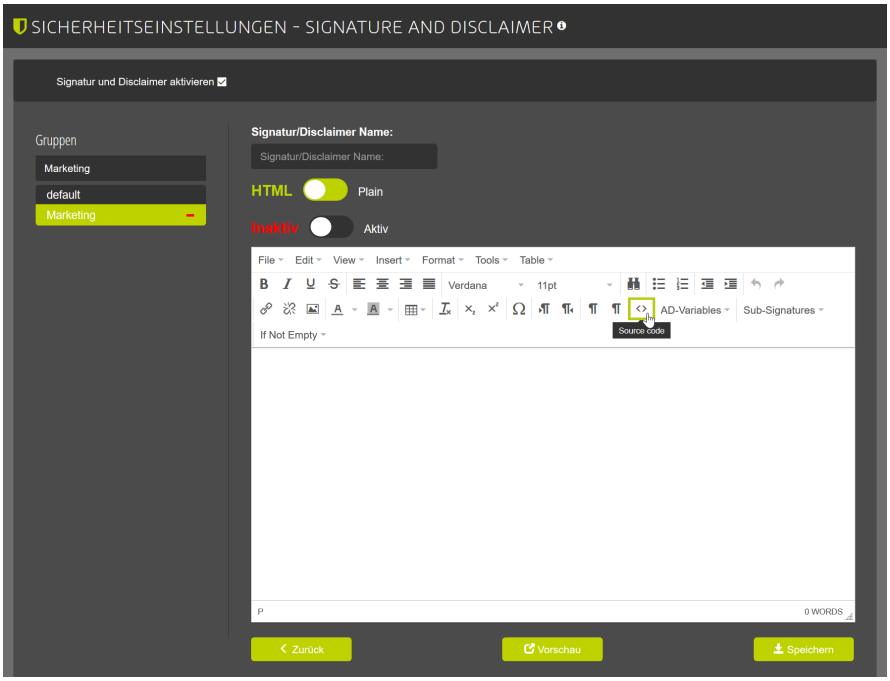


Illustration 446 : Afficher le code source

13.

REMARQUE :

Dans l'attribut **src**, saisissez le nom du champ dans lequel vous avez ajouté l'adresse graphique dans les données de base. Les noms des champs sont détaillés ci-après à titre d'exemple :

- **Département** : department
- **Nom affiché** : displayname
- **Bureau** : office
- **État** : state
- **Fax** : fax
- **Pays/région** : country
- **Localité** : city
- **Code postal** : postalcode
- **Rue, numéro** : street
- **Téléphone (professionnel)** : telephone
- **Téléphone mobile** : mobile

Saisissez un code HTML selon le modèle ci-après pour intégrer les graphiques : ****.

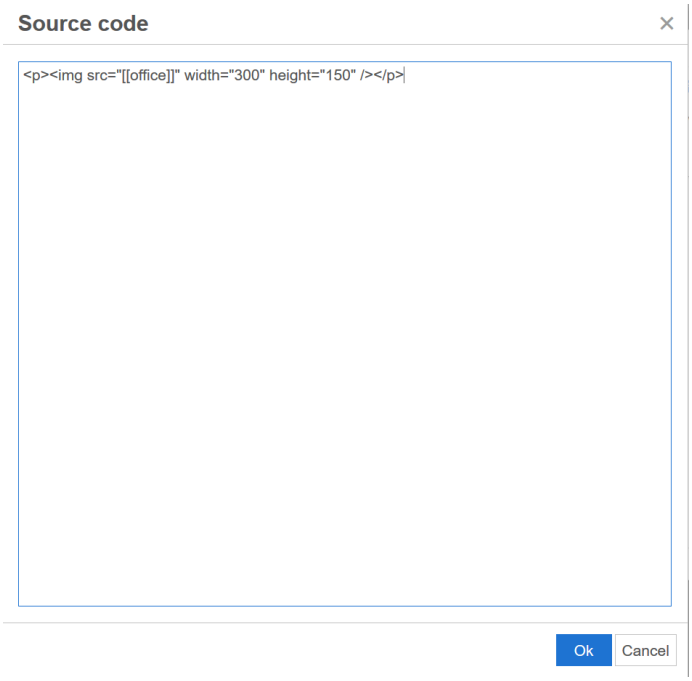


Illustration 447 : Intégration à titre d' exemple de l' adresse graphique du champ Bureau dans la fenêtre Signature

14. Cliquez sur **OK**.

La fenêtre **Source code** est fermée et la fenêtre **Signature** apparaît.

15. Facultatif : Cliquez sur le bouton **Preview** et sélectionnez la boîte aux lettres dont vous avez édité la signature en dernier lieu.

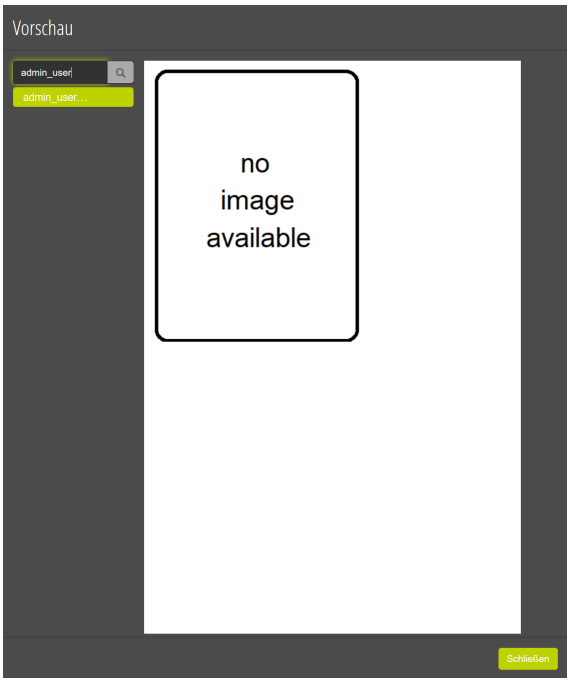


Illustration 448 : Prévisualisation de la nouvelle signature

16. Facultatif : Cliquez sur **Fermer**.

La prévisualisation se ferme.

17. Dans le champ **Signature/Disclaimer name**, saisissez un nom pour la signature que vous avez créée.

18. Cliquez sur **Save**.

La signature est enregistrée.

Différents graphiques ont été intégrés dans les signatures des différentes boîtes aux lettres d'un groupe.

Élimination des erreurs

Lors de l'utilisation de Signature and Disclaimer, des erreurs dues à une configuration défectueuse peuvent survenir. Les chapitres suivants expliquent les causes et comment corriger les erreurs courantes :

Élimination des erreurs : Les variables ne sont pas référencées

Condition :

Vous avez ajouté une variable AD ou une sous-signature (voir Intégrer des sous-signatures à la page 579) et celles-ci sont affichées incorrectement dans la signature créée.

Problème : variable AD non présente

La variable n'est pas créée dans Active Directory.

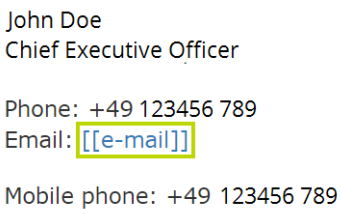


Illustration 449 : Exemple de variable AD non présente

Résolution

Sélectionnez les variables AD dans l'éditeur dans la liste déroulante.

Problème : sous-signature non présente

La signature référencée n'existe pas ou le nom de la signature a été modifié. Elle ne peut donc pas être intégrée.

Illustration 450 : Exemple pour l' intégration d' une signature non présente

Résolution

Sélectionnez la signature à intégrer à nouveau dans le menu déroulant **Sub-Signatures**.

Élimination des erreurs : Signature HTML manquante pour les courriels de Mail (Apple) ou Thunderbird

État

Les courriels envoyés par Thunderbird ou Mail (Apple) n'attachent pas la signature HTML, mais la signature simple. Si vous n'avez pas spécifié de signature pour le texte brut, le message sera envoyé sans signature.

Raison

Certains clients de messagerie comme Mail (Apple) et Thunderbird envoient des courriels par défaut sous forme de texte brut et non au format HTML. Ainsi, le modèle de texte brut est également chargé pour cela dans **Signature and Disclaimer**.

Élimination pour Mail (Apple) avec MacOS

Ouvrez Utiliser du texte non formaté et formaté dans les courriels dans Mail sur Mac et suivez les instructions du fabricant.

Workaround pour Mail (Apple) avec iOS

Dans le texte de votre courriel, formatez un ou plusieurs caractères en gras, en italique ou soulignés.

Le client envoie le courriel au format HTML et **Signature and Disclaimer** accroche la signature HTML.

Élimination pour Thunderbird

- Pour les courriels individuels : Sélectionnez **Rédiger** > **Options** > **Format de distribution** > **HTML seulement**.

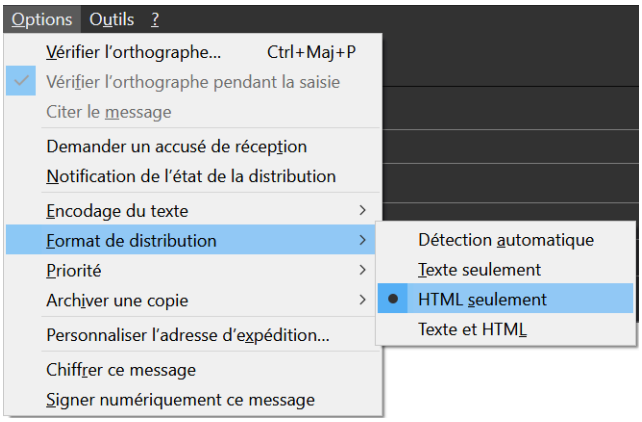


Illustration 451 : Paramètres pour un courriel individuel

- Pour tous les courriels : Sélectionnez **Rédiger** > **Extras** > **Paramètres du compte** > **Rédaction et adressage** et cochez **Rédiger les messages en HTML**.

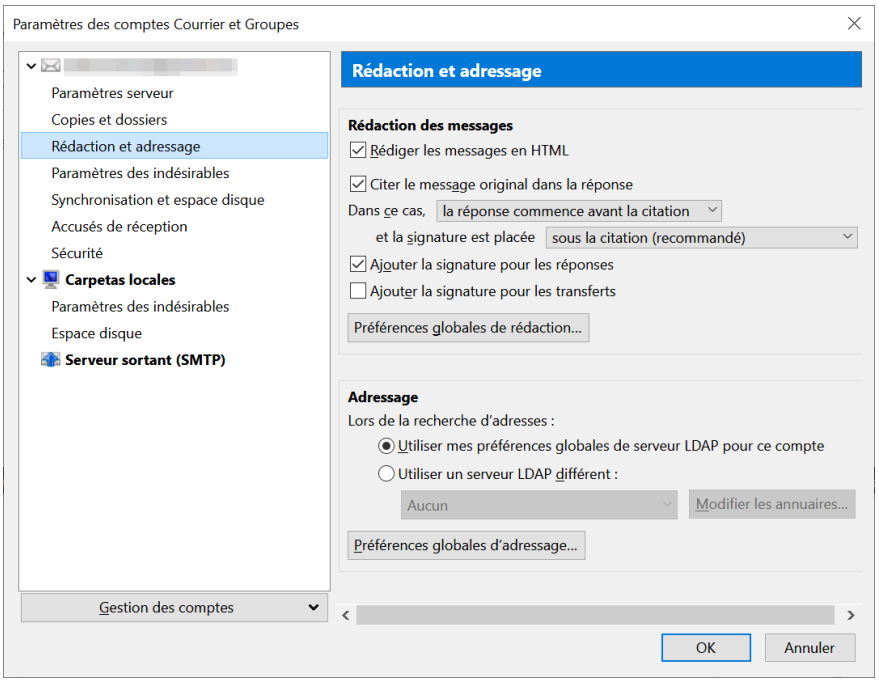


Illustration 452 : Paramètres pour tous les courriels

Élimination des erreurs : Problèmes lors de la réservation des salles dans Microsoft 365

État

Dans Microsoft 365, les salles ne peuvent plus être réservées dès que Signature and Disclaimer est activé.

Raison

Pour la réservation de salles, Microsoft 365 utilise des boîtes aux lettres spéciales, appelées boîtes aux lettres de salle, qui n'acceptent que les courriels de l'organisation propre. Dès que Signature and Disclaimer est activé, les courriels sont redirigés via nos serveurs afin que les signatures et les

clauses de non-responsabilité puissent être jointes. Les courriels qui sont redirigés via nos serveurs sont considérés comme des courriels externes et ne sont pas acceptés par les boîtes aux lettres de salle.

Résolution

1. Ouvrez Exchange Management Shell.
2. Exécutez la commande suivante :

```
Set-CalendarProcessing "" -ProcessExternalMeetingMessages $True
```

La réception de courriels externes par les boîtes aux lettres de salle est autorisée.

Continuity Service

À propos du Continuity Service

Avec le Continuity Service, les utilisateurs peuvent continuer à recevoir et à envoyer des courriels si leur propre serveur de messagerie tombe en panne. Une fois que le Continuity Service est mis en place pour un domaine ou un utilisateur individuel, le réglage par défaut est d'activer automatiquement le Continuity Service en cas de panne du serveur de messagerie.

Si les utilisateurs sont synchronisés via LDAP, il est alors nécessaire de définir un mot de passe d'urgence (voir Activer le mot de passe d'urgence) afin de pouvoir accéder au système de messagerie Web du Continuity Service.

IMPORTANT :

Le Continuity Service est un système standby. Si un client n'active le service qu'après la panne de son propre serveur de messagerie, le Continuity Service ne sera effectif qu'après un délai de plusieurs heures. Les courriels envoyés entretemps peuvent donc être perdus. Pour pouvoir maintenir de façon fiable le trafic de courriels, le Continuity Service doit être activé en permanence.

Pour les domaines dont le Continuity Service est activé, les courriels des trois derniers mois sont stockés dans les archives de courriel. Dans le module **Email Live Tracking** (voir « Email Live Tracking » dans le manuel du Control Panel), l'utilisateur peut savoir lesquels de ces courriels ont été distribués via le Continuity Service.

REMARQUE :

Les courriels qui ont été distribués via le Continuity Service ont encore le statut **Retardé** après leur distribution.

Ces possibilités de réglage du Continuity Services sont décrites ci-après :

- Activer le Continuity Service (voir Activer le Continuity Service)
- Ajouter tous les utilisateurs d'un domaine au Continuity Service (voir Ajouter tous les utilisateurs d'un domaine au Continuity Service à la page 604)
- Ajouter des utilisateurs individuels au Continuity Service (voir Ajouter des utilisateurs individuels au Continuity Service à la page 605)
- Exclure un utilisateur du Continuity Service (voir Exclure un utilisateur du Continuity Service à la page 607)
- Activer le mot de passe d'urgence (voir Activer le mot de passe d'urgence)
- Désactiver le Continuity Service (voir Désactiver le Continuity Service)

Ajouter tous les utilisateurs d'un domaine au Continuity Service

Vous avez activé le Continuity Service (voir Activer le Continuity Service).

Dans le module **Paramètres de sécurité** > **Continuity Service**, vous pouvez ajouter tous les utilisateurs d'un domaine au Continuity Service (voir À propos du Continuity Service à la page 603) pour que le trafic de messagerie de leurs boîtes aux lettres puisse être maintenu en cas de panne de votre propre serveur de messagerie.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.

3. Naviguez vers **Paramètres de sécurité** > **Continuity Service**.
4. **IMPORTANT :**

   Si vous passez de l'option **Utilisateurs sélectionnés uniquement** à l'option **Tous les utilisateurs**, tous les utilisateurs ajoutés précédemment sont supprimés.

   Pour activer le Continuity Service pour tous les utilisateurs du domaine, cochez la case **Tous les utilisateurs**.

   Si vous avez déjà ajouté des utilisateurs individuels au Continuity Service, un message d'avertissement apparaît.
5. Si un message d'avertissement apparaît, cliquez sur **Confirmer**.

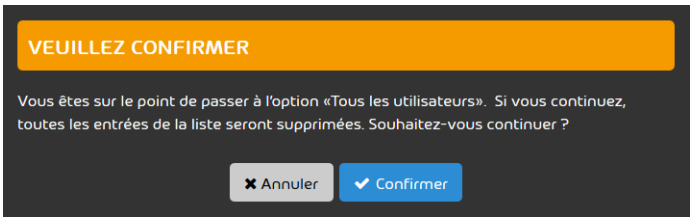


Illustration 453 : Confirmer

Le Continuity Service s'applique à tous les utilisateurs du domaine.

Tous les utilisateurs d'un domaine ont été ajoutés au Continuity Service.

Ajouter des utilisateurs individuels au Continuity Service

Vous avez activé le Continuity Service (voir Activer le Continuity Service).

Dans le module **Paramètres de sécurité** > **Continuity Service**, vous pouvez ajouter des utilisateurs individuels d'un domaine au Continuity Service (voir À propos du Continuity Service à la page 603) pour que le trafic de messagerie de leurs boîtes aux lettres puisse être maintenu en cas de panne de votre propre serveur de messagerie.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.

3. Naviguez vers **Paramètres de sécurité** > **Continuity Service**.
4. Cochez la case **Utilisateurs sélectionnés uniquement**.
5. Dans **Utilisateurs de Continuity Service**, cliquez sur **Ajouter**.

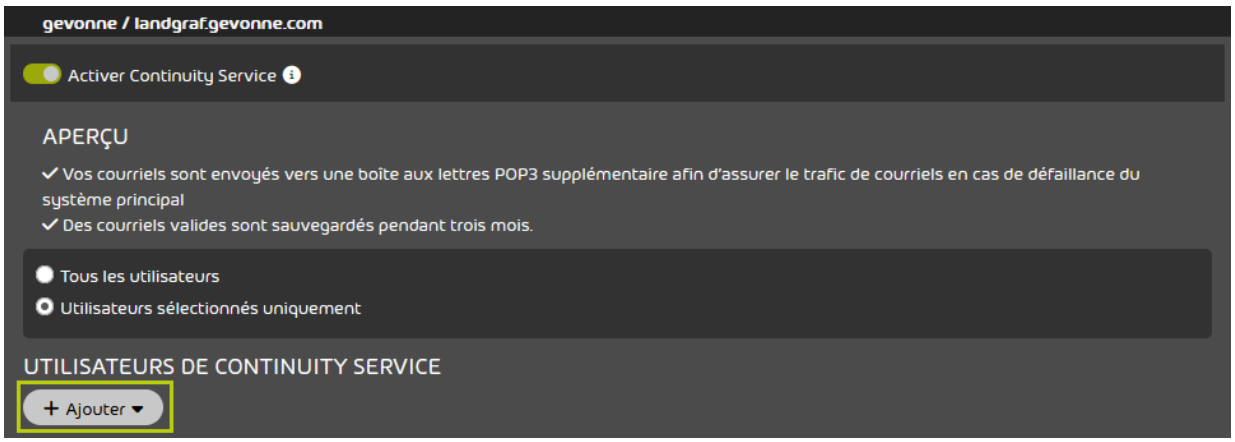


Illustration 454 : Ajouter un utilisateur

Un affichage étendu s'ouvre.

6. Sous **Sélectionner utilisateur**, saisissez l'adresse courriel de l'utilisateur que vous souhaitez ajouter.

> **REMARQUE :**
>
> Pour déclencher la fonction de proposition automatique, entrez au moins trois caractères consécutifs.

7. Cliquez sur **Ajouter**.

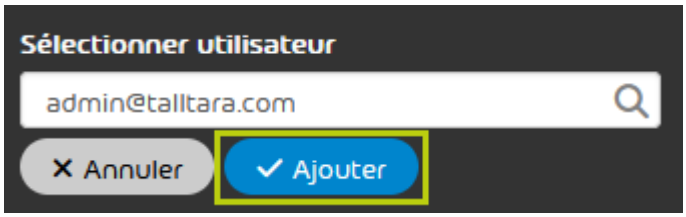


Illustration 455 : Saisir l' utilisateur

L'utilisateur est ajouté et apparaît dans le tableau. Le Continuity Service est appliqué à l'utilisateur.

Un utilisateur individuel a été ajouté au Continuity Service.

Exclure un utilisateur du Continuity Service

Vous avez ajouté des utilisateurs individuels au Continuity Service (voir Ajouter des utilisateurs individuels au Continuity Service à la page 605).

Dans le module **Paramètres de sécurité** > **Continuity Service**, vous pouvez exclure des utilisateurs afin qu'ils ne soient plus protégés par le Continuity Service.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez le domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Continuity Service**.
4. Pour exclure un utilisateur du Continuity Service, cliquez sur la croix à côté de l'utilisateur sous **Éliminer utilisateur**.

Illustration 456 : Supprimer l' utilisateur

L'utilisateur est supprimé de la liste. Le Continuity Service n'est plus appliqué à l'utilisateur.

Un utilisateur a été exclu du Continuity Service.

Personnalisation

Personnalisation du Control Panel

Dans le module **Personnalisation**, les administrateurs peuvent personnaliser le Control Panel à deux niveaux.

D'une part, les administrateurs peuvent définir l'apparence des courriels envoyés par le Control Panel (voir Adapter le modèle des courriels à la page 615), et les coordonnées qui y sont stockées (voir Adapter les informations des courriels à la page 612) et affichées.

REMARQUE :

Les notifications par courriel de Websafe (voir « Websafe » dans le manuel du Control Panel) sont également personnalisées en fonction de ces paramètres.

D'autre part, les administrateurs peuvent personnaliser graphiquement le site web du Control Panel et la Progressive Web App et définir une nouvelle URL et un nouveau nom pour celle-ci (voir Personnaliser le Control Panel à la page 618).

Les personnalisations seront affichées à tous les utilisateurs qui se connectent via le domaine saisi.

ATTENTION :

L'utilisation d'un Control Panel adapté entraîne des coûts supplémentaires selon la liste des prix.

IMPORTANT :

Si un administrateur côté client n'a pas enregistré de paramètres pour son domaine dans l'un des onglets du module **Personnalisation**, les paramètres du partenaire supérieur qui y a stocké des informations seront utilisés pour son domaine. Si aucun réglage n'est enregistré au niveau du partenaire supérieur ou de son partenaire supérieur, aucune personnalisation n'est appliquée.

IMPORTANT :

Les informations du support (voir Enregistrer les informations du support dans le Control Panel à la page 609) doivent être enregistrées, même si aucune autre option de personnalisation n'est utilisée. Les informations du support s'affichent pour les utilisateurs dans le Control Panel.

Enregistrer les informations du support dans le Control Panel

Dans l'onglet **Informations du support** du module **Personnalisation** (voir Personnalisation du Control Panel à la page 608), vous pouvez enregistrer les informations du support de votre entreprise à afficher aux utilisateurs dans le Control Panel. Ce paramètre est indépendant de la personnalisation payante du Control Panel. Les données enregistrées ici sont également affichées dans la version standard du Control Panel.

REMARQUE :

Les paramètres d'un partenaire sont également appliqués à ses sous-partenaires et clients si ces derniers n'ont pas effectué leurs propres réglages.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez effectuer les personnalisations.

3. Naviguez vers **Personnalisation** > **Informations du support**.

Illustration 457 : Sélectionner les informations du support

4. Dans le champ **Numéro de téléphone du support**, saisissez le numéro de téléphone auquel votre entreprise est disponible pour les questions d'assistance.

> **REMARQUE :**
>
> Si l'un des champs décrits ici est vide pour un client ou un partenaire, la valeur du partenaire immédiatement supérieur qui y a enregistré des informations est utilisée pour ce champ. Si ce champ est vide pour tous les partenaires de niveau supérieur, les valeurs par défaut du Control Panel sont reprises.

5. Dans le champ **Adresse e-mail du support**, saisissez l'adresse courriel auquel votre entreprise est disponible pour les questions d'assistance.

Illustration 458 : Saisir les informations du support

6. Cliquez sur **Enregistrer**.

Les informations du support ont été enregistrées dans le Control Panel.

Vous pouvez ensuite adapter les courriels envoyés par le Control Panel à votre entreprise (voir Modifier les courriels du Control Panel à la page 611) ainsi qu'adapter l'apparence du Control Panel (voir Personnaliser le Control Panel à la page 618).

Modifier les courriels du Control Panel

Le Control Panel envoie automatiquement des courriels dans différentes situations, par exemple lorsqu'un utilisateur demande un nouveau mot de passe (voir « Réinitialiser le mot de passe » dans le manuel du Control Panel). Vous pouvez adapter aussi bien l'apparence des courriels envoyés par le Control Panel que les informations qui y figurent à votre entreprise.

1. Adaptez les informations des courriels à votre entreprise (voir Adapter les informations des courriels à la page 612).

Les courriels envoyés par le Control Panel contiennent des mentions légales personnalisées, le nom de l'interlocuteur de l'entreprise ainsi qu'une adresse personnalisée de l'expéditeur.

2. Adaptez l'apparence des courriels à votre entreprise (voir Adapter le modèle des courriels à la page 615).

   La couleur des pieds de page, l'agencement des couleurs (thème) des courriels et le logo de l'en-tête des courriels sont adaptés.

L'apparence des courriels envoyés par le Control Panel et les informations qui y figurent ont été adaptées.

Vous pouvez ensuite adapter l'apparence du Control Panel (voir Personnaliser le Control Panel à la page 618).

Adapter les informations des courriels

Sous **Informations des courriels** dans le module **Personnalisation** (voir Personnalisation du Control Panel à la page 608), vous pouvez définir, pour les courriels envoyés depuis le Control Panel, une formule d'accueil, un interlocuteur, une adresse d'expédition et des informations obligatoires.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel souhaitez effectuer les ajustements.
3. Naviguez vers **Personnalisation** > **Informations des courriels**.

   Un formulaire apparaît.

Illustration 459 : Informations des courriels

4. Remplissez le formulaire. Les champs ont les significations suivantes :

   - **Nom de partenaire** : on saisit ici le nom de l'entreprise mentionné dans la salutation au début du courriel (par ex. « Cher client <Nom de l'entreprise>, »).
   - **Contact** : on saisit ici le texte de signature qui s'affiche dans les courriels sous la formule d'accueil (par ex. « L'équipe Control Panel »).
   - **Adresse d' expéditeur pour modèles de courriels** : on saisit ici l'adresse de l'expéditeur des courriels envoyés depuis le Control Panel.

     REMARQUE :

     Cette adresse d'expéditeur ne s'applique pas pour les courriels envoyés par Websafe (voir le chapitre « Websafe » dans le manuel du Control Panel).

     REMARQUE :

     Si un client a activé la vérification SPF (voir le chapitre « Activer la vérification SPF » dans le manuel du Control Panel), notre entrée SPF doit être enregistrée dans la zone DNS du domaine de l'adresse d'expéditeur (voir le chapitre « Définir un enregistrement SPF » dans le manuel du Control Panel). Autrement, les vérifications SPF des courriels envoyés par le Control Panel entraîneront des erreurs (voir le chapitre « Logique de la vérification SPF » dans le manuel du Control Panel).

   - **Nom d'expéditeur** : on saisit ici le nom affiché de l'expéditeur.
   - **Mention légale** : on saisit ici les mentions légales de l'entreprise.

     REMARQUE :

     Si l'un de ces champs est vide pour un client ou un partenaire, la valeur du partenaire immédiatement supérieur qui y a enregistré des informations est utilisée pour ce champ. Si ce champ est vide pour tous les partenaires de niveau supérieur, les valeurs par défaut du Control Panel sont reprises.

5. Cliquez sur **Enregistrer**.

Les informations des courriels ont été adaptées.

Vous pouvez ensuite adapter l'apparence des courriels envoyés par le Control Panel à votre entreprise (voir Adapter le modèle des courriels à la page 615) ainsi qu'adapter l'apparence du Control Panel (voir Personnaliser le Control Panel à la page 618).

Adapter le modèle des courriels

Dans l'onglet **Modèle de courriel** du module **Personnalisation** (voir Personnalisation du Control Panel à la page 608), vous pouvez adapter l'apparence des courriels envoyés par le Control Panel en fonction de l'image de marque de votre entreprise. La personnalisation du modèle des courriels est indépendante de la personnalisation payante du Control Panel et n'entraîne pas de coûts supplémentaires. Toutefois, lorsque vous personnalisez le Control Panel, la couleur principale, le thème et le logo de l'onglet **Modèle de courriel** sont également utilisés dans le Control Panel (voir Personnaliser l'apparence et l'URL du Control Panel à la page 620).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez effectuer les ajustements.
3. Naviguez vers **Personnalisation** > **Modèle de courriel**.

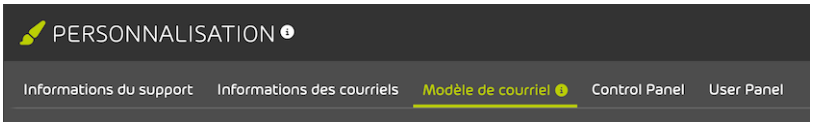


Illustration 460 : Sélectionner l'onglet

4. Sélectionnez une couleur pour le pied de page des courriels envoyés depuis le Control Panel.

   a) Cliquez sur le champ sous **Couleur primaire**.

Illustration 461 : Sélectionner une couleur

   b) Sélectionnez une couleur. Vous pouvez cliquer sur la couleur dans le champ de dégradé ou saisir le code de la couleur en HEX, RGB ou HSL dans le champ.

> **REMARQUE :**
>
> Si le Control Panel est personnalisé, la couleur sélectionnée est également utilisée comme couleur primaire pour le Control Panel (voir Personnaliser l'apparence et l'URL du Control Panel à la page 620).

La couleur sélectionnée est représentée dans le cercle et le code couleur s'affiche en HEX, RGB ou HSL.

Illustration 462 : Pied de page dans un rapport de quarantaine

5. Sélectionnez un thème pour vos courriels sous **Thème**. Vous avez deux options :

   - **Foncé** : un thème sombre est sélectionné. Les courriels sont représentés dans des couleurs sombres.

Illustration 463 : Courriel avec thème sombre

   - **Clair** : un thème clair est sélectionné. Les courriels sont représentés dans des couleurs claires.

Illustration 464 : Courriel avec thème clair

6. Cliquez sur **Parcourir** sous **Logo** et sélectionnez votre logo.

> **REMARQUE :**
>
> Un logo avec une résolution de 160 × 80 Pixel permet d'obtenir les meilleurs résultats.
>
> Seul le format de fichier .png est pris en charge.
>
> Le logo est affiché dans l'entête des courriels envoyés à partir du Control Panel.

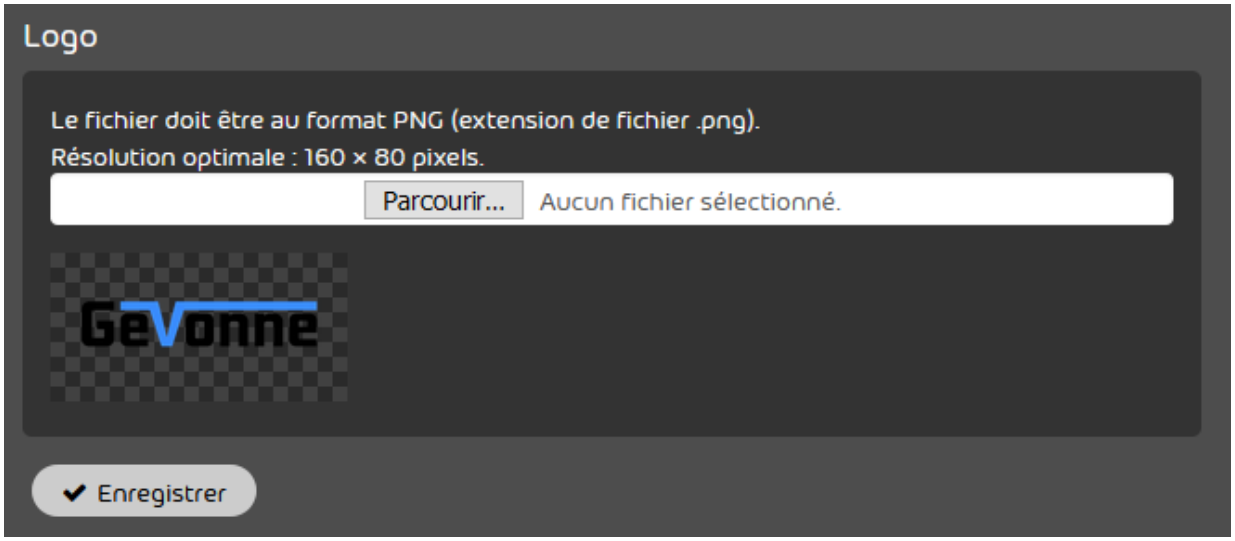


Illustration 465 : Sélectionner le logo

7. Cliquez sur **Enregistrer**.

L'apparence des courriels envoyés par le Control Panel a été adaptée.

Vous pouvez ensuite adapter les informations des courriels envoyés par le Control Panel à votre entreprise (voir Adapter les informations des courriels à la page 612) ainsi qu'adapter l'apparence du Control Panel (voir Personnaliser le Control Panel à la page 618).

Personnaliser le Control Panel

Vous pouvez adapter l'URL et l'apparence du Control Panel en spécifiant une URL de votre domaine et en y incluant les couleurs, le logo et la favicône de votre entreprise.

1. Indiquez une URL de votre domaine pour le Control Panel et configurez une redirection vers l'URL standard du Control Panel en utilisant un enregistrement CNAME dans la zone DNS de votre domaine.

   Ci-après, un enregistrement CNAME est créé pour **controlpanel.domaineclient.com** :

   controlpanel.domaineclient.com IN CNAME <URL standard>

   > **REMARQUE :**
   >
   > Vous pouvez demander l'URL standard du Control Panel au support.

2. Adaptez l'apparence et l'URL du site Web du Control Panel (voir Personnaliser l'apparence et l'URL du Control Panel à la page 620 et Adapter le modèle des courriels à la page 615).
3. Adaptez le nom et l'icône de l'application Web progressive au design de votre entreprise (voir Modifier l'application Web progressive à la page 624).
4. Enregistrez les informations d'assistance (numéro de téléphone et adresse courriel) que vous souhaitez afficher pour les utilisateurs dans le Control Panel (voir Enregistrer les informations du support dans le Control Panel à la page 609).

> **REMARQUE :**
>
> Ce paramètre est indépendant de la personnalisation payante du Control Panel. Les coordonnées enregistrées ici sont également affichées dans la version standard du Control Panel.

Illustration 466 : Coordonnées dans le Control Panel

5. **ATTENTION :**

   La création d'une version adaptée du Control Panel entraîne des coûts supplémentaires selon la liste des prix.

   PRUDENCE :

   Assurez-vous d'avoir bien saisi toutes les données dans le module **Personnalisation** ainsi que l'URL de votre Control Panel adapté.

   Pour faire adapter le Control Panel en fonction des informations et des fichiers que vous fournissez, veuillez contacter notre service d'assistance.

Le Control Panel a été personnalisé.

Personnaliser l'apparence et l'URL du Control Panel

Vous avez adapté le modèle de courriel (voir Adapter le modèle des courriels à la page 615).

Dans l'onglet **Control Panel** du module **Personnalisation** (voir Personnalisation du Control Panel à la page 608), vous pouvez personnaliser l'apparence du Control Panel en fonction de l'image de marque de votre entreprise. La couleur primaire, le thème et le logo du Control Panel personnalisé sont tirés des paramètres de l'onglet **Modèle de courriel**.

REMARQUE :

Voici quelques exemples de la manière dont les paramètres de l'onglet **Modèle de courriel** affectent le Control Panel personnalisé (voir Adapter le modèle des courriels à la page 615).

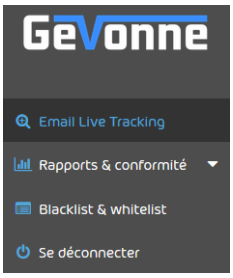


Illustration 467 : Affichage du Control Panel avec thème sombre et logo personnalisé

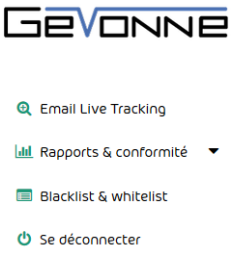


Illustration 468 : Affichage du Control Panel avec thème clair et logo personnalisé

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez effectuer les ajustements.
3. Naviguez vers **Personnalisation** > **Control Panel**.

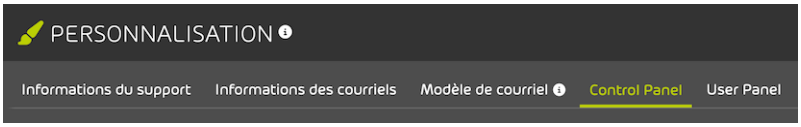


Illustration 469 : Sélectionner l' onglet

4. **IMPORTANT :**

   La personnalisation du Control Panel n'est possible que pour les partenaires ou les clients qui ont au moins 5 000 utilisateurs sous leur responsabilité.

   Actionnez le bouton **Activer la personnalisation du Control Panel**.

   Une fenêtre de confirmation apparaît.

5. **ATTENTION :**

   La personnalisation du Control Panel est payante.

   Cliquez sur **Confirmer**.

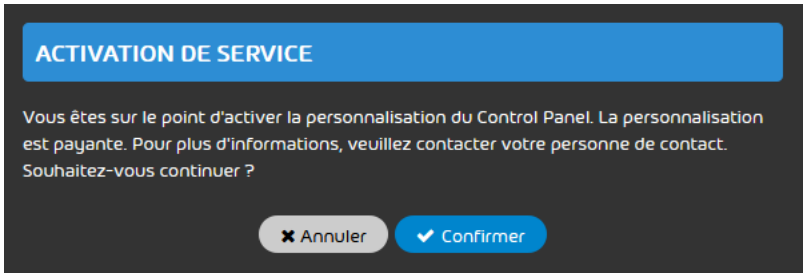


Illustration 470 : Confirmer

Les paramètres de l'onglet **Control Panel** sont activés.

6. **PRUDENCE :**

   La personnalisation du Control Panel ne fonctionne que si l'URL du Control Panel personnalisé pointe vers l'URL de la version standard du Control Panel via un enregistrement CNAME.

   Assurez-vous que l'URL pointe vers l'URL de la version standard du Control Panel via un enregistrement CNAME (voir Personnaliser le Control Panel à la page 618).

   Dans le champ **URL**, saisissez l'URL de votre domaine où vous souhaitez que votre Control Panel personnalisé soit accessible.

   L'URL doit correspondre au modèle suivant : **controlpanel.domaineclient.fr**

7. Cliquez sur **Parcourir** sous **Favicon** et sélectionnez votre favicône.

> **REMARQUE :**
>
> La favicône doit être téléchargée au format de fichier ICO (extension de fichier *.ico). L'affichage est optimal avec une résolution d'au moins 128 x 128 pixels.

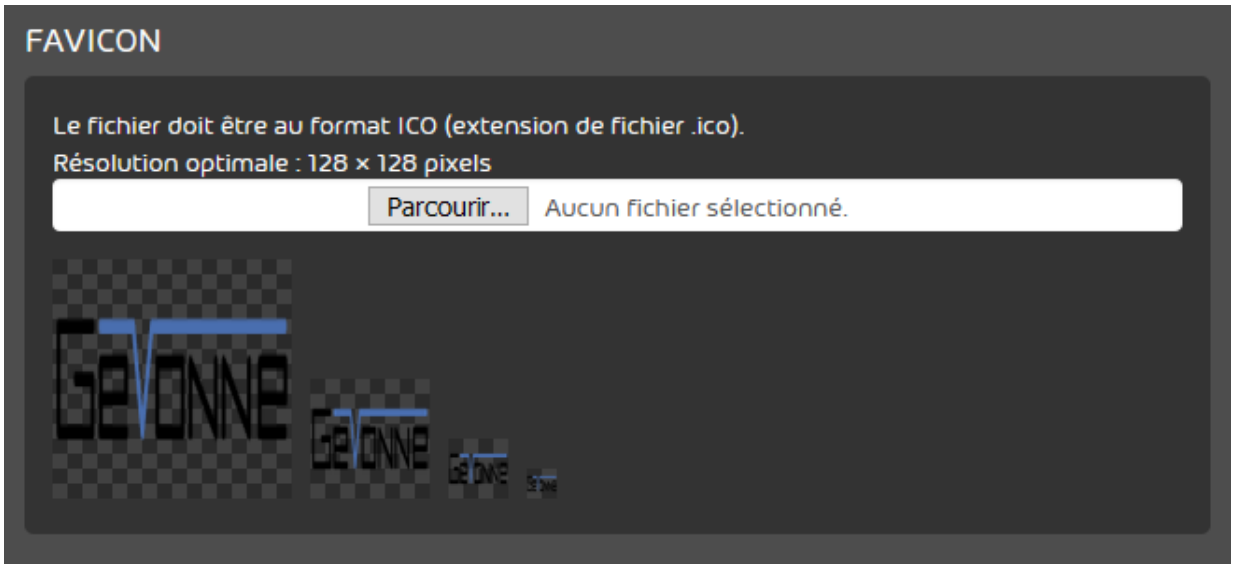


Illustration 471 : Sélectionner une favicône

8. Personnalisez la Progressive Web App (voir Modifier l' application Web progressive à la page 624).
9. Cliquez sur **Enregistrer**.

> **REMARQUE :**
>
> La mise en place de la personnalisation prend un maximum de 5 minutes.

10. Mettez à jour le site Web pour afficher vos personnalisations.

> **REMARQUE :**
>
> Les modifications sont visibles uniquement sous l'URL du Control Panel modifié.

L'apparence et l'URL du Control Panel ont été adaptées au coût.

Vous pouvez ensuite adapter l'apparence de la Progressive Web App (voir Modifier l'application Web progressive à la page 624) et enregistrer des informations de support (voir Enregistrer les informations du support dans le Control Panel à la page 609).

Modifier l'application Web progressive

Vous avez activé la personnalisation du Control Panel (voir Personnaliser l'apparence et l'URL du Control Panel à la page 620).

Dans l'onglet **Control Panel** du module **Personnalisation** (voir Personnalisation du Control Panel à la page 608), vous pouvez adapter le nom et l'icône de l'application Web progressive au design de votre entreprise.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Dans la sélection de l'espace, sélectionnez le domaine pour lequel vous souhaitez effectuer les ajustements.
3. Naviguez vers **Personnalisation** > **Control Panel**.
4. Saisissez dans **Nom de l'application** le nom qui doit apparaître sur l'écran d'accueil des appareils mobiles.

Illustration 472 : Saisir le nom de l'application

5. Téléchargez sous **Icône de l'application** une image.

> **REMARQUE :**
>
> Seul le format de fichier .png est pris en charge.

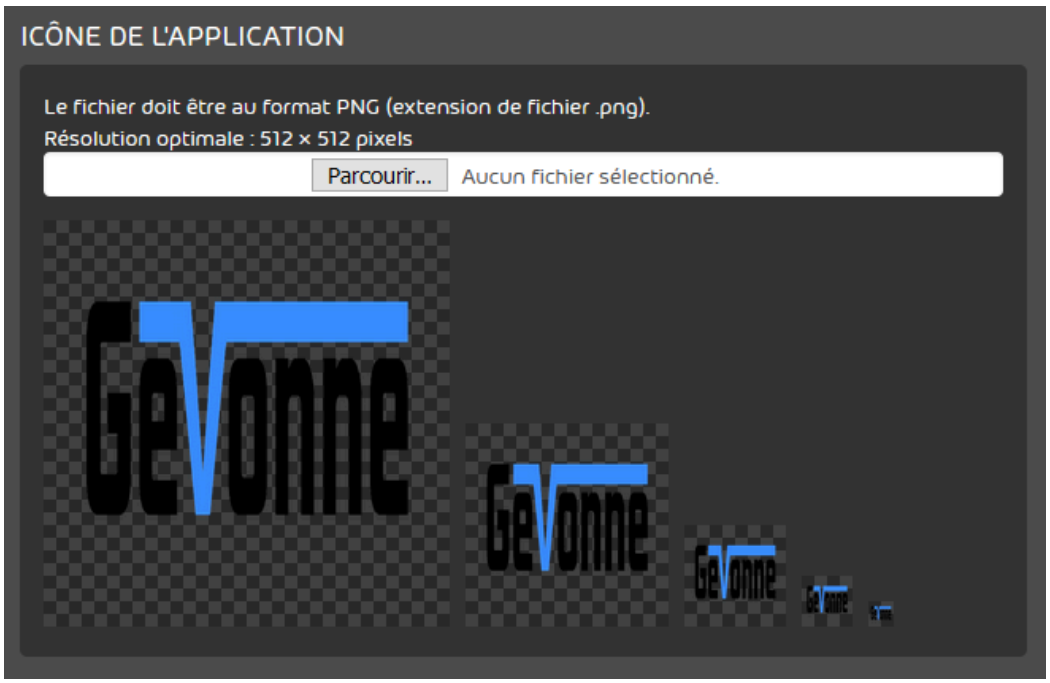


Illustration 473 : Charger l'icône de l'application

- Dans la sélection de l'icône de l'application, une prévisualisation de l'icône dans différentes tailles s'affiche. De plus, sous **Écran de démarrage**, une prévisualisation de l'écran de démarrage s'affiche. Le Splashscreen est affiché pendant le chargement de l'application Web progressive et contient le fichier image qui a été chargé sous **Logo**.

Illustration 474 : Prévisualisation du Splashscreen

6. Cliquez sur **Enregistrer**.

Le nom et le logo de l'application Web progressive ont été adaptés.

Vous pouvez ensuite adapter l'apparence du Control Panel (voir Personnaliser l'apparence et l'URL du Control Panel à la page 620) et enregistrer des informations de support (voir Enregistrer les informations du support dans le Control Panel à la page 609).

Raisons de catégorisation de courriel

Raisons de catégorisation

Chaque courriel est attribué à une catégorie dans le Control Panel (voir « Catégories de courriels » dans le manuel du Control Panel). Les raisons de la catégorisation des courriels sont indiquées dans le module **Email Live Tracking** (voir « Email Live Tracking » dans le manuel du Control Panel) dans la colonne **Raison**.

Les raisons de catégorisation sont détaillées et clarifiées avec les catégories de courriels dans le tableau suivant.

Tableau 45 : Raisons de catégorisation

RAISON	CATÉGORIE	DÉFINITION
450 4.5.5 E-Mail deferred because of Spam sending to unlock goto {URL}	Refusé	Le courriel a été refusé temporairement car le courriel indésirable a été envoyé depuis l'adresse courriel de l'expéditeur. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
450 4.5.5 too many false recipients rate-limited;	Refusé	Le courriel a été refusé temporairement car il contient un trop grand nombre de faux destinataires.

RAISON	CATÉGORIE	DÉFINITION
450 4.5.5 unblock {URL}	Refusé	Le courriel a été refusé temporairement en raison du contenu de l'en-tête. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
450 4.5.6 busy try again later;	Refusé	Le courriel a été refusé en raison d'une surcharge sur le serveur.
450 4.5.7 busy try again later by {passerelle}	Refusé	Le courriel a été refusé en raison d'une surcharge sur le serveur. Le nom d'hôte de notre passerelle est indiqué.
450 4.5.7 loop detected, by {relais};	Refusé	Le courriel a été refusé temporairement car une boucle a été détectée. Le nom d'hôte de notre relais est indiqué.
450 4.5.8 no mail data, by {relais};	Refusé	Le courriel a été refusé temporairement car il n'a aucun contenu. Le nom d'hôte de notre relais est indiqué.
450 4.5.8 no mail data;	Refusé	Le courriel a été refusé temporairement car il n'a aucun contenu.

RAISON	CATÉGORIE	DÉFINITION
450 4.5.8 too much load try next hop;	Refusé	Le courriel a été refusé temporairement en raison d'une surcharge sur le serveur. La distribution doit être testée par un autre bond.
450 4.5.9 Connection PID broken $CLEANUPID by $(hostname);	Refusé	Le courriel a été refusé temporairement en raison d'une erreur système.
450 4.5.9 Greylisted, please try again later;	Refusé	Le courriel a été refusé temporairement en raison du greylisting.
450 4.5.9 no resources please take next hop. by {relais};	Refusé	Le courriel a été refusé temporairement car aucune ressource n'est disponible pour la réception. La distribution doit être testée par un autre bond. Le nom d'hôte de notre relais est indiqué.
450 4.5.9 no smtp resources, please take next hop. by {relais};	Refusé	Le courriel a été refusé temporairement car aucune ressource SMTP n'est disponible pour la réception. Le nom d'hôte de notre relais est indiqué.
450 5.5.6 loop detected;	Refusé	Le courriel a été refusé temporairement car une boucle a été découverte.

RAISON	CATÉGORIE	DÉFINITION
454 4.7.1 [adresse courriel de l'expéditeur]: Relay access denied	Retardé	Le courriel a été retardé parce que le courriel n'a pas été envoyé depuis l'une des adresses IP des serveurs de relais du module **Spam and Malware Protection** (voir « Spam and Malware Protection » dans le manuel du Control Panel). Le client ne peut envoyer via notre infrastructure que des courriels provenant de l'une des adresses IP enregistrées. Après un jour, la distribution du courriel sera arrêtée.
504 5.5.2 Recipient address rejected: need fully-qualified address	Refusé	Le courriel a été refusé car l'adresse courriel du destinataire n'était pas complète.
523 5.2.3 E-Mail rejected, e-mail is too large by company rule [ID de règle];	Refusé	Le courriel a été refusé car il dépasse la taille autorisée définie côté client. L'ID de règle est indiqué.
550 5.1.1 Recipient address rejected: undeliverable address	Refusé	Le courriel a été refusé car l'adresse courriel du destinataire n'existe pas.

RAISON	CATÉGORIE	DÉFINITION
552 5.2.2 Mailbox not available. For more information visit {URL};	Refusé	Le courriel a été refusé en raison de l'adresse courriel du destinataire ou de l'expéditeur. Le nom d'hôte de notre passerelle est indiqué.
552 5.5.2 Message size exceeds fixed maximum message size. Size: {taille du courriel}, Max size: {taille maximale} by {passerelle};	Refusé	Le courriel a été refusé car il dépasse la taille limite sur la passerelle. Le nom d'hôte de notre passerelle est indiqué.
552 5.5.2 Size: {taille du courriel}	Refusé	Le courriel a été refusé conformément aux directives du Content Control (voir « À propos du Content Control » dans le manuel du Control Panel) car il ne respecte pas les restrictions de taille en vigueur. La taille du courriel est indiquée.
552 5.5.8 utilize Smarthost instead of MX by {passerelle};	Refusé	Le courriel a été refusé car il doit être expédié via un Smarthost et non pas directement à la passerelle. Le nom d'hôte de notre passerelle est indiqué.

RAISON	CATÉGORIE	DÉFINITION
554 5.5.4 Your IP {adresse IP} address has a bad reputation. To unblock visit {URL};	Refusé	Le courriel a été refusé car votre adresse IP a une réputation négative. Vous pouvez déverrouiller votre adresse courriel en accédant à l'URL indiquée.
554 5.5.5 E-Mail rejected Spam found, for support contact {URL};	Refusé	Le courriel a été refusé car il contient un courriel indésirable. Pour soumettre une demande au support, accédez à l'URL indiquée.
554 5.6.0 unblock {URL};	Refusé	Le courriel a été refusé en raison de la taille trop importante de l'en-tête. Pour soumettre une demande au support, accédez à l'URL indiquée.
554 5.6.1 E-Mail rejected because of Spam-Header to unlock goto {URL};	Refusé	Votre courriel a été refusé car il a été identifié comme un courriel indésirable en raison de l'en-tête. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.

RAISON	CATÉGORIE	DÉFINITION
554 5.6.1 Your mailheader contains SPAM. To unblock visit {URL}	Refusé	Votre courriel a été refusé car il a été identifié comme un courriel indésirable en raison de l'en-tête. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
554 5.6.2 E-Mail rejected because of Spam-http-Link to unlock goto {URL};	Refusé	Le courriel a été refusé car il a été identifié comme un courriel indésirable en raison d'un lien. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
554 5.6.2 Your mail contains a SPAM-LINK. To unblock visit {URL};	Refusé	Le courriel a été refusé car il a été identifié comme un courriel indésirable en raison d'un lien. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
554 5.6.3 E-Mail rejected because of Spam-Body to unlock goto {URL};	Refusé	Le courriel a été refusé car il a été identifié comme un courriel indésirable en raison de son texte. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.

RAISON	CATÉGORIE	DÉFINITION
554 5.6.3 Your mail contains SPAM. To unblock visit {URL};	Refusé	Le courriel a été refusé car il contient un courriel indésirable. Vous pouvez déverrouiller l'adresse courriel en accédant à l'URL indiquée.
554 5.6.4 E-Mail rejected, forbidden attachment by company rule Attachments {ID de règle}	Refusé	Le courriel a été rejeté car il contient une pièce jointe interdite par les règles du client. L'ID de règle est indiqué.
554 5.6.4 E-Mail rejected Virus found, for support contact {URL}	Refusé	Le courriel a été rejeté car il contient des virus. Pour soumettre une demande au support, accédez à l'URL indiquée.
554 5.6.9, customer rule based reject by antispameurope Compliancfilter ID-{ID de règle}	Refusé	Le courriel a été refusé par la règle du Compliance Filter indiquée (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle est indiqué.
554 5.6.9 Compliance rule based reject by antispameurope Compliancefilter ID-{ID de règle} by {passerelle};	Refusé	Le courriel a été refusé par la règle du Compliance Filter indiquée de l'hôte indiqué (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle et le nom d'hôte de notre passerelle sont indiqués.

RAISON	CATÉGORIE	DÉFINITION
554 5.6.9 Compliance rule based reject by Compliancefilter ID-{ID de règle} by {passerelle};	Refusé	Le courriel a été refusé par la règle du Compliance Filter indiquée de l'hôte indiqué (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle et le nom d'hôte de notre passerelle sont indiqués.
554 5.7.0 Sender address rejected: {adresse de l'expéditeur} sending out spam;	Refusé	Le courriel a été refusé car l'expéditeur a envoyé un courriel indésirable.
554 5.7.12 SPF fail by customer policy. {passerelle};	Refusé	Le courriel a été refusé en raison d'un échec SPF suite à un paramétrage côté client (voir « Vérification SPF » dans le manuel du Control Panel). Le nom d'hôte de notre passerelle est indiqué.

RAISON	CATÉGORIE	DÉFINITION
554 5.7.1 Domain / User unknown	Refusé	Le courriel a été refusé car le domaine indiqué ou la boîte aux lettres indiquée n'est pas disponible dans le Control Panel (voir « Domaines » dans le manuel du Control Panel et « Boîtes aux lettres » dans le manuel du Control Panel). **REMARQUE :** La création ainsi que la synchronisation de nouvelles boîtes aux lettres peuvent durer jusqu'à 90 minutes. Si des courriels sont envoyés à une boîte aux lettres avant que sa création ne soit terminée, les courriels seront rejetés.
554 5.7.2 Sender address rejected: Access denied;	Refusé	Le courriel a été refusé car l'adresse IP de l'expéditeur n'est pas enregistrée par nos services.

RAISON	CATÉGORIE	DÉFINITION
Allowed by User Policy	Valide	L'expéditeur ou l'hôte expéditeur du courriel a été autorisé par le destinataire (voir « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel).
Bad Host Reputation	Spam	L'hôte expéditeur du courriel a une réputation négative.
Bad IP Reputation	Spam	L'adresse IP de l'hôte expéditeur du courriel a une réputation négative.
Bad Sender Reputation	Spam	L'expéditeur du courriel a une réputation négative.
Bad URL Reputation	Spam	Le courriel contient au moins un lien vers un serveur Web ayant une réputation négative.
Block by Compliance Filter Policy ID-{ID de règle}	Refusé	Le courriel a été bloqué par une règle du Compliance Filter en tant que Threat (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle est indiqué.
Business Email Compromise	AdvThreat	Le courriel est un courriel malveillant avec un faux expéditeur de votre propre entreprise.

RAISON	CATÉGORIE	DÉFINITION
Clean by Compliance Rule ID-{ID de règle}	Valide	Le courriel a été classé comme valide par une règle du Compliance Filter (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle est indiqué.
Denied by User Policy	Spam	L'expéditeur ou l'hôte expéditeur du courriel a été interdit par le destinataire (voir « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel).
Detached by Content Control Policy	Contenu	Au moins une pièce jointe n'est pas autorisée en raison des paramètres du Content Control (voir « À propos du Content Control » dans le manuel du Control Panel).
DKIM Failure	Spam	La validation DKIM a échoué (voir « Validation DKIM et signature DKIM » dans le manuel du Control Panel).
DMARC Failure	Spam	La validation DMARC a échoué (voir « Validation DMARC » dans le manuel du Control Panel).

RAISON	CATÉGORIE	DÉFINITION
Envelope SPF Failure	Refusé , Spam	La vérification SPF dans l'enveloppe du courriel a échoué (voir « Vérification SPF » dans le manuel du Control Panel). **Rejeter le courriel** ou **Enregistrer le courriel comme spam en quarantaine** a été défini comme une action suite à une erreur.
Good Sender Reputation	Valide	L'expéditeur ou l'hôte expéditeur du courriel a une réputation positive.
Ham	Valide	Ham est l'opposé du courriel malveillant. Il s'agit d'un courriel désiré qui correspond au modèle d'un courriel valide.
Impersonation attempt by customer policy	AdvThreat , Threat	Le nom affiché de l'expéditeur du courriel est le même que le nom affiché d'un utilisateur saisi dans le Control Panel, mais l'adresse courriel dans l'en-tête (From) est différente de celle saisie pour cet utilisateur.

RAISON	CATÉGORIE	DÉFINITION
infomail	Infomail, Spam	Le courriel est probablement une infolettre. Soit l'expéditeur ou la plage d'adresses IP de l'expéditeur du courriel est une source connue d'infolettres, soit le courriel contient des mots-clés, des chaînes de caractères ou d'autres caractéristiques dont la combinaison indique qu'il s'agit d'une infolettre.
Malicious Attachment	AdvThreat , Refusé, Threat	Au moins une pièce jointe du courriel est malveillante.
Malicious Email Content	AdvThreat , Refusé, Threat	Le courriel contient du contenu malveillant.
Malicious URL	AdvThreat , Refusé, Threat	Le courriel contient des liens vers des sites Web ou des documents malveillants.
Massive Attack Prevention	AdvThreat , Threat	Le courriel correspond au modèle d'une campagne de lancement de logiciels malveillants.

RAISON	CATÉGORIE	DÉFINITION
Message Header SPF Failure	Refusé , Spam	La vérification SPF dans l'entête du courriel a échoué (voir « Vérification SPF » dans le manuel du Control Panel). **Rejeter le courriel** ou **Enregistrer le courriel comme spam en quarantaine** a été défini comme une action suite à une erreur.
Phishing	AdvThreat , Threat	Le courriel contient les caractéristiques d'une attaque de phishing.
RBL	Refusé	L'hôte expéditeur du courriel a une réputation négative.
Rejected by Content Filter	Contenu	Le courriel a été refusé conformément aux directives du Content Control (voir « À propos du Content Control » dans le manuel du Control Panel) car il contient au moins une pièce jointe interdite.

RAISON	CATÉGORIE	DÉFINITION
Sandbox	AdvThreat	Au moins une pièce jointe du courriel a été soumise à une analyse dynamique par le moteur Sandbox d'Advanced Threat Protection et évaluée comme malveillante (voir « Description des moteurs ATP » dans le manuel du Control Panel).
Sender Allowed by Domain Policy	Valide	L'expéditeur ou l'hôte expéditeur du courriel a été autorisé par l'administrateur du client (voir « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel).
Sender Denied by Domain Policy	Spam	L'expéditeur ou l'hôte expéditeur du courriel a été interdit par l'administrateur du client (voir « À propos des expéditeurs interdits et autorisés » dans le manuel du Control Panel).

RAISON	CATÉGORIE	DÉFINITION
Spam by Compliance Rule ID-{ID de règle}	Spam	Le courriel a été classé comme courriel indésirable par une règle du Compliance Filter (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle est indiqué.
Spam Content	Spam	Le courriel contient des contenus classés comme courriel indésirable.
SPF Failure	Refusé	Le courriel a été refusé en raison d'un échec SPF (voir « Vérification SPF » dans le manuel du Control Panel).
Statusmail	Valide	Le courriel est une notification système générée automatiquement, ,par ex. un rapport de quarantaine (voir « À propos du Quarantine Report » dans le manuel du Control Panel).
Targeted Fraud	AdvThreat	Le courriel correspond au modèle d'une attaque malveillante ciblée.

RAISON	CATÉGORIE	DÉFINITION
Threat by Compliance Rule ID-{ID de règle}	Threat	Le courriel a été classé par une règle du Compliance Filter en tant que Threat (voir « À propos du Compliance Filter » dans le manuel du Control Panel). L'ID de règle est indiqué.
Unsolicited Email	Spam	Le courriel a été évalué comme indésirable car il contient notamment une offre non sollicitée.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com