Dialog Insight

Catalyseur d'intelligence marketing

Configurations initiales à l'ouverture du compte

Configurations initiales

2019.03.05

Canada • France • Russie

dialoginsight.com

Table des matières

Configurations de base

Introduction

Ce document décrit les configurations que Dialog Insight vous recommande de faire dès l'ouverture de votre compte.

Ces configurations ont pour objectif d'*authentifier* correctement vos envois (c'est-à-dire, prouver que les messages transmis par la plateforme proviennent de votre entreprise) et faciliter l'utilisation par vos employés.

Nous recommandons d'effectuer les configurations suivantes pour assurer une saine gestion de vos envois :

- L'authentification de vos envois (DKIM et DMARC)
- L'utilisation d'un domaine personnalisé pour les liens suivis
- L'inscription des serveurs de Dialog Insight sur votre liste blanche

Importance de l'authentification des envois

L'authentification des envois est ce qui permet de différencier les messages légitimes de message indésirable qui utiliserait votre domaine. Une bonne configuration prouve à vos destinataires que vos messages sont légitimes et aide à bloquer les messages qui ne le sont pas.

Une bonne authentification vous permet aussi d'établir votre réputation d'envoyeur, contribue à augmenter vos taux de livraison, réduit les risques que vos messages soient filtrés et classés comme pourriels et à augmenter la confiance de vos destinataires envers vos communications électroniques.

À l'inverse, ne pas authentifier vos messages vous expose à des risques. Si un serveur de réception ne peut prouver qu'un serveur a le droit de transmettre des messages en votre nom, vous vous exposez aux conséquences principales suivantes :

- Il sera plus difficile de créer et maintenir une bonne réputation d'envoyeur, et cette réputation peut être facilement endommagée par une campagne de pourriels exploitant la réputation de votre domaine ;
- Vos destinataires pourraient être avisés que les messages « ne semblent pas provenir réellement de vos domaines », ou que l'origine du message ne peut être confirmée ;
- Vos domaines pourraient facilement être exploités par des campagnes d'hameçonnage, puisque qu'il n'est pas possible de différencier vos messages légitimes de ceux qui ne le sont pas.

Il existe deux façons d'authentifier les envois :

- Par signature DKIM
- Par protocole SPF

Mais ce n'est pas tout. Il faut savoir que même si la signature DKIM ou le protocole SPF aident à prouver qu'un message est légitime, leur absence ou échec ne prouvent pas l'inverse.

Par conséquent, il est important de mettre en place une politique DMARC pour pallier à cette incertitude et indiquer explicitement ce qui doit être fait avec un message non authentifié.

Authentification des envois par signature DKIM

La signature DKIM (« DomainKeys Identified Mail ») est un standard Internet qui est presqu'universellement supporté par les fournisseurs de courriels et systèmes anti-spam majeurs.

L'approche utilisée par DKIM est de valider que le message est autorisé par le propriétaire du domaine de l'expéditeur du message via l'ajout d'une *signature digitale* au message.

Cette signature est basée sur une paire de clés de cryptographie :

- le signataire (Dialog Insight dans ce cas) possède la partie *privée* de la clé, qui sert à signer les messages,
- la partie *publique* de la clé est inscrite dans les DNS du domaine pour lequel les messages sont signés.

À la réception d'un message, un serveur de réception qui trouve une signature consultera les serveurs DNS pour récupérer la clé publique et utilisera cette clé pour valider la signature.

Une signature validée prouve 2 choses :

1. Le message a été signé par un serveur (Dialog Insight) qui possède la clé privée. Il est donc autorisé à signer par le propriétaire du domaine (votre entreprise), puisque la présence de la clé publique dans vos DNS prouve que vous avez accepté que DI signe pour vous;
2. Le message n'a pas été altéré en transit. Si le message avait été modifié, la signature ne serait plus valide.

Mise en place d'une signature DKIM dans la plateforme Dialog Insight

Pour mettre en place les signatures DKIM pour vos domaines, vous devez :

1. Répertorier tous les domaines qui seront utilisés comme adresse d'expéditeur dans vos messages (par exemple : « votreentreprise.com » et « service.votreentreprise.com »)
2. Transmettre une demande d'obtention de signatures DKIM à notre équipe de support, en indiquant la liste des domaines répertoriée.
3. Créer les entrées DNS qui seront fournies par notre équipe dans les domaines fournis, et aviser notre équipe lorsqu'elles sont faites.

Notre équipe validera ensuite les entrées et activera les signatures DKIM pour ces domaines dans votre compte.

Pour en savoir plus sur DKIM : http://www.dkim.org/

Authentification des envois par protocole SPF

SPF (acronyme de « Sender Policy Framework ») est un protocole qui permet de déterminer si un message provient d'un serveur autorisé à utiliser un nom de domaine particulier pour livrer des messages, en comparant son adresse IP à une liste d'adresses publiées dans les DNS du domaine de *l'enveloppe SMTP* du message.

L'enveloppe SMTP, c'est comme l'adresse de retour inscrite sur une enveloppe postale : une adresse potentiellement différente de celle inscrite en entête de la lettre qui se trouve à l'intérieur de l'enveloppe.

La configuration du protocole SPF est optionnelle puisque Dialog Insight prend en charge le SPF par défaut si vos envois se font à partir de nos adresses mutualisées.

Si vous utilisez des adresses IP dédiées, ou si vous souhaitez que les messages transmis sur nos adresses mutualisées soient plus directement rattachés à votre domaine pour la gestion de la réputation, notre équipe technique pourra alors vous assister à configurer le SPF.

Comme pour le DKIM, il faudra alors transmettre à notre équipe technique la liste des domaines expéditeurs que vous utilisez et des entrées DNS vous seront fournies en retour. Une fois les entrées faites et validées, la configuration sera activée par notre équipe.

Validation de l'authentification par DMARC

Qu'est-ce qu'une politique DMARC

DMARC est un acronyme pour « Domain-based Message Authentication, Reporting & Conformance ».

La mise en place d'une politique DMARC permet à un envoyeur d'indiquer que leurs messages sont protégés par DKIM et/ou SPF, et indique aux serveurs de réception ce qui devrait être fait lors de la réception d'un message non-authentifié – par exemple, rejeter le message ou le classer comme indésirable.

DMARC élimine l'incertitude à la réception : bien que SPF et DKIM aident à prouver qu'un message est légitime, leur absence ou échec ne prouvent pas l'inverse.

Votre politique DMARC comble cette incertitude en vous permettant d'indiquer explicitement ce qui doit être fait avec un message non-authentifié.

Mise en place d'une politique DMARC pour votre entreprise

Le site https://dmarc.org contient toutes les ressources nécessaires pour permettre à votre équipe de comprendre DMARC, de préparer une politique appropriée, et de la tester.

Certains outils plus techniques sont aussi listés dans cette section : https://dmarc.org/resources/deployment-tools/

DMARC vs Dialog Insight

Bien que DMARC soit une politique d'entreprise son fonctionnement repose sur une bonne configuration technique des divers systèmes qui transmettent des courriels en utilisant vos domaines incluant les vôtres, ceux de Dialog Insight, ainsi que ceux de tout autre partenaire ou système transmettant des messages en votre nom.

Pour déployer une politique DMARC sécuritaire qui rejette les messages qui échouent l'authentification, il est nécessaire que tous les messages soient authentifiés correctement.

Si vous appliquez les configurations décrites aux étapes précédentes de ce guide, les envois de la plateforme Dialog Insight seront authentifiés correctement et respecteront votre politique DMARC.

Liens de suivi personnalisés

Dialog Insight capture des statistiques sur les liens cliqués dans les messages et présente aussi certains formulaires automatiquement à vos contacts (notamment : les formulaires de désabonnement ou fonctionnalités pour consulter un message en ligne).

Pour se faire, les liens que vous placez dans vos messages sont remplacés par des liens vers les serveurs de la plateforme.

Lorsque votre contact clique sur un lien, ce lien dirige d'abord aux serveurs de Dialog Insight (où le clic est journalisé) avant d'être redirigé à la destination finale (sur votre site).

À la base, ces remplacements se font en utilisant un nom de domaine associé à la plateforme (par exemple : app.dialoginsight.com).

Vos contacts pourraient trouver ces liens suspects : pourquoi un lien dans un message dirige-t-il à app.dialoginsight.com? Ils ne connaissent pas ce domaine et ne l'associent certainement pas à votre entreprise.

Pour mettre vos destinataires en confiance et réduire les risques de plaintes d'hameçonnage, il est important de configurer un nom de domaine qui sera utilisé pour personnaliser les liens de suivi.

Choisissez un *sous-domaine* du domaine principal de votre entreprise (celui que vos clients connaissent et associent à votre entreprise). Par exemple : « communications.votreentreprise.com ».

Ce nom de domaine sera utilisé pour les liens dans les messages et les divers formulaires de la plateforme auxquels vos contacts sont exposés, ce qui permettra un suivi des statistiques tout en conservant des liens associés à votre entreprise.

Mettre en place un domaine pour les liens personnalisé

Vous devez créer une entrée DNS de type CNAME qui réfère au domaine principal de l'application. La valeur exacte de l'entrée dépend de la plateforme DI à laquelle votre compte est assigné :

- Au Canada, utilisez « `secure.ofsys.com.` »
- En France, utilisez « `secure.mydialoginsight.com.` »

Une fois l'entrée DNS créée, tapez ce nom de domaine dans un navigateur. Si la configuration est correcte, vous serez redirigé à la page de connexion de la plateforme.

Finalement, pour activer ce domaine, il suffit de l'ajouter à la plateforme (sous Gestion du compte > Domaines) en tant que domaine par défaut pour l'entreprise.

Inscription des serveurs Dialog Insight sur votre liste blanche

Dans le cours normal de l'utilisation de la plateforme Dialog Insight, vous transmettrez éventuellement le même message à répétition à des adresses courriel internes à votre entreprise.

Que ce soit pour faire des tests répétitifs de messages en préparation ou des notifications automatiques intégrés dans des processus, ces scénarios génèrent des messages à haut débit, souvent vers la même adresse, et avec des contenus presque identiques.

Il est possible que vos serveurs de courriel voient ces messages répétitifs comme étant des courriels indésirables et les bloquent.

Il est aussi possible que vos systèmes antipourriels reconnaissent l'adresse de l'expéditeur comme étant une adresse qu'ils contrôlent normalement et qu'ils jugent donc inacceptable qu'un message de l'externe provienne d'une de ces adresses.

Pour éviter cette situation il est préférable de *whitelister* les messages provenant de la plateforme dans vos systèmes anti-spam pour vous assurer que ces messages arrivent à bon port.

La méthode exacte pour ajouter nos serveurs à vos listes blanches varie selon les serveurs courriels utilisés, mais la méthode idéale consiste à accepter tous les messages qui proviennent de nos réseaux (selon les adresses IP). Dialog Insight livre présentement des courriels à partir d'adresses dans les réseaux suivants :

Plateforme Canadienne : 208.91.248.0/22

Plateforme Française : 104.254.152.0/21

À éviter

Notez qu'il n'est pas conseillé de configurer vos systèmes afin qu'ils acceptent automatiquement tout message provenant de votre propre nom de domaine : c'est une erreur commune qui est systématiquement exploitée par les spammeurs / hameçonneurs qui savent que plusieurs systèmes mal configurés acceptent automatiquement des messages de leur propre domaine, sans aucune autre validation.

Configurations supplémentaires recommandées

Boucle de rétroaction des plaintes

Une *boucle de rétroaction* * est un processus commun utilisé par plusieurs fournisseurs majeurs de courriel (Hotmail, etc.) pour alerter automatiquement un expéditeur lorsqu'un destinataire porte plainte suite à la réception d'un message (typiquement via des fonctions de style « ceci est un spam »).

Dialog Insight gère automatiquement ces boucles de rétroactions et, via des ententes avec la majorité des fournisseurs qui supporte cette fonction, est automatiquement inscrit pour recevoir ces alertes dès qu'un message est livré à partir d'un de nos serveurs.

À l'exception de Yahoo! …

Une exception notable est Yahoo! : ils ne permettent pas de s'y inscrire par serveur ou adresse IP mais plutôt par nom de domaine; chaque expéditeur doit donc inscrire ses domaines chez Yahoo!.

L'inscription doit être faite par le propriétaire du domaine : le processus d'inscription exige que la personne qui s'inscrit prouve qu'elle est propriétaire du domaine inscrit.

De plus, la boucle de rétroaction de Yahoo! est basée sur la signature DKIM utilisée : aucune rétroaction ne sera donnée sur les messages qui ne sont pas signés correctement.

Avant de s'inscrire il faut donc s'assurer qu'une signature DKIM est en place pour vos domaines, et qu'un certain volume d'envoi ait eu lieu afin que Yahoo! puisse valider le domaine.

Notez qu'en plus de s'appliquer à tous les domaines Yahoo! (Yahoo.com, Yahoo.ca et autres), Yahoo! gère aussi les services courriels de plusieurs fournisseurs d'accès internet (par exemple : Rogers.ca) dans différents pays.

S'inscrire est donc important.

Autrement, les plaintes spam de tous ces domaines ne seront pas traitées et avec le temps votre réputation d'envoyeur envers Yahoo! sera en déclin, ce qui rendra de plus en plus difficile les livraisons rapides et correctes vers ces contacts.

Consultez la section en annexe qui explique comment s'inscrire à la boucle de rétroaction Yahoo!.

** La boucle de rétroaction sera plus souvent décrite avec son nom anglais (« Complaint Feedback Loop » ou simplement « Feedback Loop ») chez les fournisseurs de courriels. Soyez donc à l'affût de ce terme, qui est rarement traduit en français.*

Adresses IP dédiées (sur demande seulement)

Communiquez avec votre directeur de compte pour mettre en place une adresse IP dédiée ou pour en savoir davantage sur celles-ci.

Introduction

Initialement, vos envois sont effectués à partir d'un groupe d'adresses IP partagées entre les différents clients de Dialog Insight. Ces adresses maintiennent une excellente réputation, grâce à une surveillance continue de la part de Dialog Insight.

L'utilisation de ces adresses partagées vous permet dont de bénéficier immédiatement d'une bonne réputation pré établie auprès des principaux fournisseurs Internet.

Réputation de l'expéditeur

Cette réputation est un facteur critique dans la livraison de courriels. Au sens large, l'effet de la réputation est simple : meilleure est votre réputation, plus il sera facile (et rapide) de livrer des courriels. À l'inverse, une mauvaise réputation peut nuire à la livraison de vos messages, allant d'un débit limité à un blocage complet de vos messages.

Les courriels livrés sont observés et mesurés par une variété d'outils, et des réseaux centralisés ont été établis afin de mesurer la réputation des envoyeurs de façon collaborative.

Il existe plusieurs systèmes qui suivent la réputation des envoyeurs :

- Les principaux fournisseurs de services de courriel (Microsoft, Google, Yahoo) utilisent tous leur propre système collaboratif pour établir la réputation des envoyeurs.
- De plus en plus d'entreprises utilisent le service d'une entreprise tierce pour le filtrage de leurs courriels entrants, et ces services incluent généralement un système de réputation collaboratif (ex : Barracuda).

Selon les systèmes, cette réputation est mesurée et associée à l'adresse IP utilisée ainsi qu'au domaine de l'adresse courriel de l'expéditeur du message.

Pourquoi utiliser une adresse IP dédiée ?

L'utilisation d'adresses IP dédiées vous permet de faire vos envois dans un environnement entièrement isolé dans lequel vous êtes le seul acteur responsable de la performance et de la réputation de vos envois.

Si les communications que vous transmettez sont critiques, et que vous ne pouvez pas vous permettre le risque potentiel d'un envoi qui serait affecté par les actions d'un autre utilisateur de ces adresses, c'est le scénario idéal.

En effet, en utilisant une adresse IP dédiée à votre entreprise, vous ne subirez jamais les conséquences d'un mauvais comportement des autres clients de Dialog Insight.

Mise en place des adresses IP dédiées

Dialog Insight analysera vos envois et vous proposera le meilleur plan de mise en place d'adresses dédiées, qui tiendra compte de plusieurs facteurs dont :

- Le nombre d'adresses requises, en fonction de vos volumes d'envois, types de communications et de clientèles,
- Le plan de transition en fonction de vos fréquences et quantités d'envois pour entrainer vos nouvelles adresses et transiger des adresses partagées vers les adresses dédiées

Avant d'être utilisées, les adresses IP doivent être configurées correctement. Une partie de la configuration est faite par Dialog Insight, une autre doit être faite par votre équipe technique.

Dialog Insight vous guidera au travers de ces étapes, vous fournira toutes les entrées DNS et autres configurations requises pour la mise en place de ces adresses, et vous aidera à valider la configuration.

Autres ressources

Cette section présente des informations utiles pour la gestion de vos communications.

Surveillance de votre réputation d'expéditeur

Faire le suivi de la réputation de vos adresses est un facteur important de la réussite de vos campagnes. Une mauvaise réputation est non seulement nuisible à la livraison de vos messages, mais est aussi une indication d'un problème de fond.

En effet, une fois établie, votre réputation ne diminuera pas à moins de problèmes importants, comme un taux d'erreur de livraison très élevé à long terme sans que ces adresses soient retirées de vos listes, un trop grand nombre de plaintes de pourriel, un contenu problématique qui est généralement reconnu comme du pourriel, etc.

Bien que Dialog Insight maintienne une surveillance générale de toutes les adresses assignées à ses clients, et vous alerte si des problèmes majeurs sont détectés, il est tout de même recommandé que vous procédiez vous aussi à la surveillance de la réputation de vos adresses.

Voici quelques exemples de systèmes de réputation collaboratifs qui permettent au public de consulter votre la réputation d'expéditeur :

- Talos Intelligence : https://talosintelligence.com/reputation_center
- SenderScore : https://www.senderscore.org

Gestion de vos contacts : Désabonnements, erreurs et plaintes

Une érosion de votre base de données avec le temps est inévitable, peu importe la qualité initiale de votre liste de contacts ou de votre relation avec ces contacts.

Au fil du temps, vos contacts changent d'emploi ou de fournisseur de services et ainsi changent d'adresse courriel. D'autres perdent leur intérêt envers votre contenu et ne désirent simplement plus le recevoir.

Peu importe la raison, il est toujours très important pour vous de réagir rapidement à ces situations, pour deux raisons majeures :

1. Un taux d'erreur élevé affecte négativement votre réputation, ce qui peut mener à un déclassement de vos messages ou, à la limite, à leur rejet;
2. Des contacts qui demandent de ne plus recevoir vos communications utiliseront les fonctionnalités de plainte antipourriel si vous poursuivez l'envoi de ces communications, ce qui nuira à votre réputation.

Dialog Insight fournit plusieurs outils pour automatiser ou faciliter le traitement de ces situations.

Désabonnement

La meilleure façon de gérer les désabonnements est de laisser la plateforme Dialog Insight le faire pour vous.

La plateforme fournit deux manières de gérer les désabonnements :

- Par l'entremise d'un formulaire de désabonnement interactif géré par la plateforme, qui permet un désabonnement global ou à la pièce, ou
- Par l'entremise des fonctions de désabonnement offertes par certains logiciels courriels ou appareils mobiles, qui transmettent automatiquement la demande de désabonnement à la plateforme.

Ces désabonnements sont gérés automatiquement, sans intervention de votre part.

Notez les points suivants :

- Le désabonnement n'arrête pas tous les types d'envois
  Certains envois unitaires (par exemple les fonctionnalités virales du type « envoi à un ami ») utilisent des méthodes d'envoi différentes qui ne sont pas liées aux consentements de votre projet. Il en va de même pour les envois de types *administratifs*, qui ne sont pas assujettis aux fonctions de désabonnement normales. Il est de votre responsabilité de configurer correctement vos types de communications pour respecter les préférences de vos contacts.

- Plusieurs internautes ne font pas confiance aux liens de désabonnement
  Attendez-vous donc à recevoir des demandes de désabonnement par d'autres canaux et assurez-vous de les honorer. Facilitez la tâche à vous utilisateurs en vous assurant que l'adresse de l'expéditeur de vos messages est une adresse valide (pas de « noreply@... »), que les réponses envoyées seront lues et traitées promptement.

Certains clients préfèrent gérer les consentements dans leur propre plateforme et optent donc pour un processus de désabonnement maison. Si vous choisissez cette approche :

- Assurez-vous que le processus d'accès au profil est le plus simple possible.
- Notez aussi que si vous transmettez des messages assujettis à certaines législations (ex : LEPI/C-28 au Canada, CAN-SPAM aux États-Unis, RGPD en Europe), le processus de désabonnement est souvent réglementé. Au Canada par exemple :
  - Vous ne pouvez pas demander à la personne de se connecter à un profil pour se désabonner;
  - Vous devez honorer le désabonnement dans un délai maximal prévu par la loi.
- Certains désabonnements se produiront quand même dans la plate-forme Dialog Insight (via les fonctionnalités de plaintes et de désabonnement automatique dans les agents courriels), et vous devrez les respecter même si vous gérez les consentements dans vos systèmes.

  Considérez par exemple la fonctionnalité *Webhook* pour transmettre ces désabonnements à vos serveurs.

Considérez aussi qu'au-delà de la réglementation, exiger un mot de passe pour accéder à une fonction de désabonnement augmente considérablement le taux de plaintes!

Vos destinataires choisiront toujours la manière la plus facile de cesser de recevoir un message. Plusieurs choisiront le bouton « ceci est un spam » au lieu de se connecter à un profil qui demande un mot de passe (qu'ils auront possiblement oublié).

Évidemment, ces plaintes affectent directement votre réputation d'expéditeur.

Erreurs de livraisons et mise en quarantaine

Une gestion adéquate des erreurs de livraison est un élément clé : un taux d'erreur élevé affecte négativement votre réputation, ce qui aura des effets divers sur vos livraisons incluant :

- Des ralentissements ou blocages temporaires de vos messages,
- Un déclassement des messages (qui pourraient alors apparaitre dans la boite de courriels indésirables),
- Ou même un rejet ou effacement immédiat à la réception.

Votre taux d'erreur doit idéalement se tenir sous la barre des 1%.

Pour atteindre ce taux il est essentiel de bien gérer les erreurs de livraisons et d'épurer constamment les mauvaises adresses de vos listes.

Dialog Insight prend en charge l'essentiel de cette gestion pour vous via l'entremise de son système de *mise en quarantaine* des contacts.

Qu'est-ce que la mise en quarantaine ?

Lorsqu'un contact est mis en quarantaine, il n'est plus éligible à recevoir des courriels.

Ce statut est temporaire et indépendant des consentements : dès que l'adresse courriel du contact est modifiée (que ce soit par un import, un utilisateur ou par le destinataire lui-même via un formulaire de profil), la quarantaine sera levée et le système reprendra automatiquement les envois, avec les consentements originaux du contact.

Mise en quarantaine des adresses invalides

La mise en quarantaine vise d'abord les adresses courriels qui sont *confirmées* invalides. Il s'agit ici d'erreurs très précises et irréversibles, où nos serveurs ont contacté le serveur à destination et ont obtenu une réponse claire qui nous assure que cette adresse n'existe pas.

Il s'agit de cas très précis, par exemple :

- Un serveur qui fournit un message standard de type « Delivery Status Notification » avec un code d'erreur spécifique, ou
- Des codes ou réponses standardisées de certains logiciels ou systèmes de filtrage spécifiques (ex : Barracuda, Office 365, …), ou
- Des réponses sur mesure gérées spécialement pour les fournisseurs de courriels majeurs (Yahoo, Gmail, Orange, …)

Pour ces cas, la mise en quarantaine est immédiate. Votre liste sera donc épurée rapidement si des mauvaises adresses sont utilisées.

Mise en quarantaine lors d'erreurs répétitives

Au-delà des erreurs qui mènent à une mise en quarantaine immédiate, plusieurs autres types d'erreurs de livraison peuvent se produire.

Une boite courriel peut être pleine, un message particulier peut être rejeté par un filtre antipourriel à cause de son contenu, un serveur peut être en panne pendant quelques jours.

Ces erreurs ne justifient pas le retrait systématiquement d'un contact de vos listes d'envoi.

Ces cas deviennent un problème lorsque la situation persiste. Considérez par exemple une boite courriel *abandonnée* par son utilisateur, qui est pleine et le restera à vie (ou jusqu'à ce que le fournisseur ferme automatiquement le compte).

Il existe aussi d'autres cas d'erreurs permanentes qui ne sont pas reconnues immédiatement par la plate-forme : bien que le processus de mise en quarantaine immédiate détecte une grande majorité des cas et qu'il soit en constante évolution pour détecter de nouveaux cas, il y aura toujours des serveurs moins bien configurés pour lesquels les messages d'erreurs sont imprécis et ne permettent pas une mise en quarantaine immédiate.

Pour éviter de continuer à transmettre des messages à des destinataires invalides (ce qui affecterait votre réputation), Dialog Insight effectue une surveillance des contacts pour lesquels des erreurs répétitives se produisent, sans aucune livraison réussie entretemps.

Un contact sera aussi placé en quarantaine :

- Après au moins 7 erreurs de livraison consécutives,
- Et ce sur une période d'au moins 45 jours.

Cette configuration par défaut est volontairement très conservatrice mais peut être ajustée pour mieux correspondre au contexte de votre entreprise et de vos envois.

Annexe 1

Boucles de rétroaction Yahoo (FeedbackLoop, FBL)

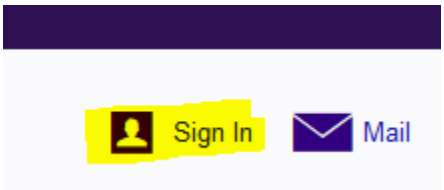
La personne qui fait la demande doit avoir accès en temps réel aux messages transmis au *postmaster* du domaine pour lequel la demande est faite (i.e. le domaine qui sera utilisé dans les adresses d'expéditeur des messages de Dialog Insight).

Exemple : postmaster@votredomaine.com

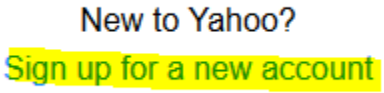
Il est recommandé de tester l'envoi d'un message à cette adresse au préalable pour être certain qu'ils sont bien reçus car, même si la mise en place d'une adresse postmaster est requise selon les standards, ce n'est pas tous les domaines qui honorent cette spécification ou qui savent clairement où vont ces messages.

Compte Yahoo (YahooID)

La demande doit se faire à partir d'une identité Yahoo. Une identité Yahoo peut se créer au besoin à partir du lien « ***Sign In*** », en haut à droite des pages du site Yahoo.com :



Et en suivant le lien « ***Sign up for a new account*** » qui se trouve dans le formulaire de connexion :

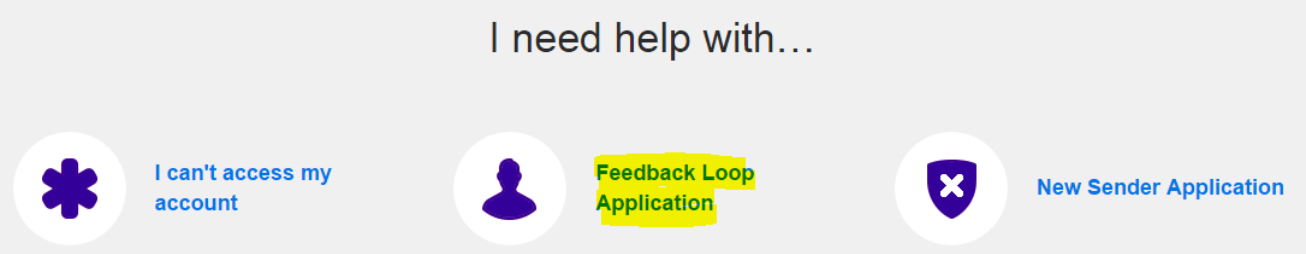


Il s'agit d'une procédure de création de compte standard comme on en retrouve sur tous les autres sites web.

Formulaire de demande

La demande se fait à partir de cette page : https://help.yahoo.com/kb/postmaster/

Il faut suivre le lien « ***Feedback Loop Application*** » en entête :



Le formulaire demande :

- Des coordonnées générales sur le client
- Les informations nécessaires pour choisir quels rapports sont à transmettre (les champs ***Domain*** et ***Selector***)
- L'adresse à laquelle livrer les rapports

En plus de fournir vos coordonnées, vous devez entrer l'information suivante dans les champs ci-dessous :

- ***Reporting Email*** : (depend de la plateforme, voir ci-dessous)
- ***Selector*** : (dépend du « selector » dans les clés DKIM qui vous ont été fournies)
- ***Request type*** : Add
- ***Domain*** : Le nom de domaine à inscrire

La valeur pour ***Reporting EMail*** est une adresse courriel dans notre plateforme qui reçoit les rapports de Yahoo!. La valeur dépend de la plateforme :

- Au Canada, utiliser yahoo@feedback.ofsys.com
- En France, utiliser yahoo@feedback.mydialoginsight.com

Domain est le domaine des adresses d'expéditeur des messages de Dialog Insight que vous envoyez. C'est le domaine pour lequel nous voulons recevoir les plaintes. Si vous envoyez des messages à partir de plusieurs domaines (ou plusieurs sous-domaines d'un même domaine), vous devez soumettre ce formulaire pour chaque domaine.

Finalement, le ***Selector*** identifie quelles signatures nous intéressent : nous voulons recevoir les plaintes qui suivent des envois en provenance de Dialog Insight seulement (nous ne pouvons pas traiter d'autres plaintes que celles-là), donc on inscrit ici le ***Selector*** qui a été choisi par Dialog Insight lorsque les entrées DNS pour le DKIM ont été faites. Nous utilisons généralement « DI » comme ***Selector***, ce qui permet de reconnaître facilement nos signatures (il se pourrait dans certains cas que le ***Selector***

soit différent, dans un tel cas la bonne valeur vous sera fournie à l'ouverture du compte).

Vérification de la demande

Le bouton « Get Verification Code » envoie un message à postmaster@votredomaine.com

Ce code doit être saisie dans la page suivante avant de soumettre la demande, i.e. il faut le faire en temps réel (on ne peut pas revenir plus tard avec le code, et le message ne contient que le code, pas un lien qui permet de venir compléter).

Une fois le code saisi, et la demande soumise, il y a ensuite un délai de 48 heures avant que la demande soit traitée.

Contact
Canada : 1 866 529-6214
France : +33 (0) 1 86 76 69 96

Courriel : info@dialoginsight.com
Site Web : www.dialoginsight.com
Blogue : www.dialoginsight.com/fr/ressources/academie

@DialogInsight
Dialog Insight