Dialog Insight

Smart Marketing Catalyst

Dialog Insight

Initial Configurations

4/21/2016

Canada • France • Russia

dialoginsight.com

Table of Contents

Basic Configurations

Introduction

When setting up an account, the following elements should be configured by the client as soon as possible to improve message delivery, reduce anti-spam reports and phishing attempts, and to facilitate the message testing process.

The following three elements must be configured:

- Your domain and sub-domain SPF entries
- Personalized follow-up links
- Whitelisting OFSYS servers

SPF Entries

SPF entries are used for two main validation types: SPF validations and SenderID validations (mostly used by Hotmail / Microsoft).

SPF entries correspond to DNS entries that are published as TXT records.

SPF entries must be applied to all domain and sub-domain names that could be used in the sender's email address when sending messages through the OFSYS applications.

For example:

If you send messages using the following addresses:

newsletter@yourcompany.com

info@service.yourcompany.com

You will need to provide one SPF entry for the domain name "yourcompany.com" and one SPF entry for the sub-domain name "service.yourcompany.com".

The SPF entry must list all the email servers that can deliver messages on your behalf. The SPF entry must therefore be configured properly for your company as well as for Dialog Insight.

A typical SPF entry looks like this:

"v=spf1 mx include:ofsys.com -all"

If you already have SPF entries set up, you will just need to add the "include:ofsys.com" part to your existing entry. However, if you don't have any entry set up, we strongly recommend that your technical team becomes familiar with this standard and to publish corresponding SPF entries for all domains and sub-domains from which you plan to send messages (even if they are not used by the OFSYS application), as not doing so will expose your company to phishing attempts and will harm your sender reputation, which in turn will affect the proper delivery of your messages.

Please refer to the following websites to get further information on setting up SPF entries:
http://old.openspf.org/wizard.html
http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/

The following websites are used to validate existing entries:
http://www.kitterman.com/spf/validate.html
http://www.openspf.org/Why

Personalized Follow-Up Links

Dialog Insight can collect usage statistics on links clicked in sent messages by adding its own servers between your contacts and your servers, so that when a contact clicks on a link, it is first registered in Dialog Insight (to be logged) and then automatically delivered to its final destination.

Links in your messages are therefore converted and use by default Dialog Insight's domain name (ofsys.com). In order to help message recipients associate the content to your company (which reduces possible phishing complaints), it is recommended to configure a sub-domain of your company's domain (i.e. newsletter.yourcompany.com). This sub-domain name will be used for all links and contents in your messages that must refer to our servers.

Note that a sub-domain must be used, such as **sub-domain**.domain.com, and not a sub-folder, such as http://domain.com/**sub-folder**).

Here are some valid examples:

- http://newsletter.yourcompany.com
- http://contest.yourcompany.com

ARE NOT valid, nor functional, the following examples:

- http://yourcompany.com/newsletter
- http://www.yourcompany.com/contest

In addition, A CNAME type DNS entry must be created on the client's DNS servers for this sub-domain, and the CNAME entry must refer to ofsys.com. For example:

newsletter.yourcompany.com CNAME ofsys.com

An easy way to test if your DNS entry is valid once the record has been created is to type the sub-domain name in a Web browser (ex: http://newsletter.yourcompany.com). If configuration was properly done, you should be redirected to the Dialog Insight login page.

Whitelisting OFSYS servers

In the course of your normal use of OFSYS tools, you are bound to repetitively send the same message to internal email addresses, such as for testing a newsletter you are creating.

And these repetitive messages might be considered as spam by your servers and even be deleted.

It is also possible that your anti-spam systems recognize the sender's address as one they usually control and therefore consider inappropriate that an external message originates from one of these addresses.

To facilitate your work, it is suggested that you set up your email filter systems to automatically unblock message originating from our servers to make sure your tests can be run and sent correctly.

The exact process to add our servers to your white lists varies according to the email servers your use.

Filtering can be based on the domain name of the server that delivers your messages (*.ofsys.com), on the email address of the SMTP envelope (*@ofsys.com), or simply the server's IP address. For the latest, the following IP address can be used to deliver messages:

208.91.248.0/22

Additional Configurations (On Demand Only)

Introduction

Apart from the basic configuration elements, many additional configurations are possible to further improve your message delivery processes. These configurations however are only available on demand and must be performed by your technical team in collaboration with Dialog Insight.

Contact your account manager to know more about these settings or to implement any of these configuration elements.

Dedicated IP Addresses

Shared Addresses

By default, your messages are sent from a group of IP addresses that are shared amongst Dialog Insight's clients. These IP addresses provide you with an impeccable sender reputation and enable Dialog Insight to constantly monitor this reputation, thus making your message deliveries benefit from a predefined and immediate good reputation with major Internet providers.

Why Use Dedicated IP Addresses?

The use of dedicated IP addresses lets you send messages in a completely secure environment, in which you are the only person responsible for the performance and reputation of your deliveries. If your communications are crucial and you cannot risk having consequences related to the use of this address by others, a dedicated IP address is ideal. In fact, by using an IP address dedicated to your company, you will never be affected by the behavior of other Dialog Insight clients.

Your Sender's Reputation

Email messages delivered are validated and measured using a variety of tools, and centralized networks have been set to measure senders' reputation on a collaborative basis.

There are various collaborative systems:

- Major email service providers, such as Hotmail, Yahoo, AOL, and Gmail, all use a certain number of these systems, or equivalent internal systems.
- More and more companies use a third-party company to filter their incoming emails, who generally offer a reputation system.

The sender's reputation is a key element in the delivery of messages; in fact, whatever the content of the message is, a bad reputation can literally block all your messages even before that reach standard anti-spam validation systems.

Depending on the systems, this reputation is measured and associated to the domain of the email address of the sender of the message.

How Many IP Addresses Can Be Assigned?

Unless particular circumstances, it is always better to limit as much as possible the number of IP addresses used. For the majority of senders, one IP address is sufficient, as adding more IP addresses usually reduces the delivery volume too much, thus making it more difficult to establish the good reputation.

However, multiple ID addresses can be required in specific situations, based on the following parameters:

- The relation between the desired delivery speed, your contact distribution by domain and the volume of your daily message deliveries
- The potential distribution by client type (clients vs members, for example)
- The potential distribution by communication type (promotions vs operations vs viral message deliveries)

Dialog Insight will validate with you your needs and will determine whether one or more IP addresses should be used.

Configuring IP Addresses

Before being used, IP addresses must be configured correctly. Part of this configuration is done by Dialog Insight, and another must be done by your technical team.

Client's DNS Entries

A domain name is assigned to, and identifies, each IP address, and is used by Dialog Insight's servers when connecting with other servers to deliver messages.

In order to show that the IP address is connected to the client's company, the domain name assigned should use a name that can easily be associated with you and known by your clients. The domain name can then be prefixed to clearly identify each IP address, in a format similar to the following:

- mta1.yourcompany.com

If you have been assigned multiple ID addresses, a sequential count of each "MTA" (standard acronym of "Mail Transport Agent") will be used.

For each of these domain names, a series of DNS entries will need to be created on your DNS servers:

- SPF Entry
  This record indicates that the address is authorized to deliver messages for this specific domain name.
- MX Entry
  This entry indicates to which server messages addressed to this domain should be delivered. In this context, these are automatic messages to manage delivery errors, and the target server is a Dialog Insight server designated for this use.
- A Entry
  This entry is the main entry that identifies the domain name to the assigned IP address.

Dialog Insight's DNS Entries

Once all client DNS entries are created and validated, Dialog Insight needs to create the reverse DNS entries for each IP address, which will be used to confirm that the client's IP addresses have been properly assigned.

Putting IP Addresses Online

IP address reputation measurement systems also include validations on volume variations over time. These systems are often suspicious when IP addresses suddenly start to send a very large amount of messages, as this is frequently related to computers infected by virus or Trojan, to be then transformed into zombies sending malicious emails.

Putting new IP addresses online is a delicate process that must be done gradually, usually over multiple weeks.

This process is entirely performed by Dialog Insight. A launching period is planned to send increasing numbers of messages from your dedicated addresses. Extra messages will be sent from already trained shared addresses.

Depending on the situation, a different strategy might be preferred to establish the initial reputation of your addresses. For example, if you plan on sending only one monthly message, your sender reputation will be difficult to build. In such a situation, sending your message over a few day period will be more beneficial.

After a few weeks, all your messages will be sent from your dedicated IP addresses, and the online process will be considered to be complete.

Monitoring Your Sender's Reputation

Following up on your addresses' reputation is an important factor in the success of your campaigns. A bad sender reputation not only harms the delivery of your messages, but also indicates a fundamental problem.

In fact, once established, your reputation will not decrease, unless important problems, such as a very high delivery error rate over a long period without removal of these addresses, a much too high number of spam complaints, content that is usually recognized as spam, etc.

Although Dialog Insight performs general monitoring of all addresses assigned to its clients, and informs concerned clients of major problems when they are detected, it is recommended that you also check the reputation of your addresses.

Following are a few examples of public collaborative reputation monitoring systems to check your reputation as a sender:

- Trusted Source, from Secure Computing (http://www.trustedsource.org/)
- SenderBase, from IronPort (http://www.senderbase.org/)
- SenderScore, from ReturnPath (https://www.senderscore.org/register/)

Authentication of your sender's domains

Description

In addition to your sender reputation, servers that receive your messages will also try to validate if you have given Dialog Insight the permission to deliver messages on your behalf. This validation is based on the domain of the email address used to send the message, and uses two main protocols to do so: SenderID and DKIM.

For these two validation processes, you must publish DNS entries that allow target message servers to recognize your message delivery rules. These entries must be created for all the domains that will be used to send messages.

SenderID Protocol

Microsoft' s SenderID Framework, mainly used by Hotmail and its related services (Live, MSN), uses the SPF entries of the domain of the author of the message to identify which IP addresses are authorized to deliver the message.

An SPF entry is published as a TXT type DNS record and must provide the list of all email servers that are authorized to deliver messages to the domain name. The entry must therefore be properly configured for your company and also include Dialog Insight's servers.

A standard SPF entry looks like this:

v=spf1 mx ip4:1.2.3.4 include:ofsys.com -all

where:

- **`mx`** indicates that the domain's inbound email server can also deliver messages,
- **`ip4:1.2.3.4`** indicates that the IP 1.2.3.4 address can deliver messages (this is usually your dedicated address by Dialog Insight),
- **`include:ofsys.com`** is useful during the launching process to identify the Dialog Insight's shared addresses that can deliver excess messages during your dedicated address training,
- **`-all`** indicates that no other address can deliver messages for this domain.

Important Notice: The above SPF entry is only an example and should never be used as such.

Signature DKIM

The DKIM signature (DomainKeys Identified Mail) is an Internet standard that is increasingly supported. The message validation ignores the server that made the delivery, and is rather based on a cryptographic signature that confirms that the message has not been altered in the delivery process and that the sender has the private encryption key used to produce the domain signature.

In order to authorize Dialog Insight to produce DKIM signatures on behalf of your domain, a special pair of keys is produced by Dialog Insight: the private key is kept on Dialog Insight's servers and the public key is given to you and must be added to your DNS servers.

Dialog Insight uses the private key to create and add the cryptographic signature to every message sent. This signature will then be used to prove the legitimacy of the message on destination.

For more information on this standard, visit the following site:
http://www.dkim.org/

Contact Management – Opt-outs, Errors and Complaints

The erosion of your contact list is inevitable over time, no matter how well your list was set up or how good your relation is with your contacts.

Some people change jobs or service providers, causing a change in their email address. Others loose interest in your content and choose not unsubscribe.

But whatever the reason, it is always important that you react quickly to these changes, mainly for the following two reasons:

1. A high error rate has a negative impact on your reputation – and over 10% of errors, the situation is critical and your messages could be rejected.
2. Contacts who have asked not to receive your communications anymore will usually report them as spam if you continue to send them those communications.

Dialog Insight provides multiple tools to automate or facilitate solutions for these situations, but ultimately, part of the work needs to be done manually.

Opt-out Links

The Dialog Insight Contact application includes an opt-out mechanism that automatically deactivates contacts who click on the opt-out link provided in a message and confirm the opt-out. This process is easily managed by the system. However, some additional elements must be taken into account:

- Opt-out is only applied at the current project
  So if you use multiple projects to deliver your messages, it will be your responsibility to ensure that these opt-outs are also applied to other appropriate projects. Furthermore, if you use additional sending tools, it will probably necessary for you to transfer the opt-out information to your central databases.
- Opting-out does not block other types of messages to be sent
  For instance, Tell-A Friend functions and viral invitations to surveys use different mailing process that are not linked to projects and therefore, are not affected by opt-outs. The only way to stop these other types of mailings is to put the concerned email addresses on the company's black list (or kill file).

- A lot of people do not trust opt-out links
  Expect to receive opt-out requests by email, and make sure to honor them. Help your contacts by making sure the sender's address provided in messages is valid (no "noreply@..."), and read and reply quickly to these requests.

Some companies prefer using their own opt-out process, especially when their contact lists are managed by another application, and/or when contact profiles are more sophisticated and offer multi-type subscription management.

Make sure that if you choose this approach, that the way you access contact profiles is as simple as possible. Note also that if you send messages that are subject to Canada's anti-spam law (CASL), the opt-out must be performed in one single click; you cannot ask contacts to connect to their profiles and enter a password for them to unsubscribe.

You must also take into consideration the fact that accessing profiles using passwords will highly increase the number of complaints, as users always choose the easiest way to unsubscribe, and reporting a message as spam is much easier than accessing a profile and possibly having to retrieve a password. Furthermore, these complains will directly affect your sender's reputation.

Delivery Errors

A proper management of delivery errors is crucial to maintain a good reputation. An error rate that reaches 10% is serious and can ruin your reputation. So it is essential to closely monitor deliver errors and to constantly remove problematic addresses from your list.

Dialog Insight offers two different tools to help your manage errors: automatic quarantine of bad addresses and manual management of delivery errors.

Quarantine

The quarantine process is automated in Dialog Insight when delivery errors occur. In general, servers that communicate with Dialog Insight's servers provide clear responses that apply commonly established standards, and these responses allow us to exactly identify the type of error involved.

If the identified error is considered to be irreversible (a proof that the server does not accept message for this email address), then the contact is placed in quarantine. A quarantined contact is set to be inactive and remains inactive until its email address is corrected. This process is completely transparent to the user, but tools exist to view the list of quarantined contacts or for lifting the quarantine manually if needed.

The quarantine process uses a pessimistic approach, meaning that address is put in quarantine only if it is certain that the address is invalid. Quarantine will be set if ALL the following conditions are present:

- Our servers must explicitly establish a communication with the destination server, and receive a response following a delivery attempt.
- The response must let us establish that the address is invalid based on either of the following criteria:
    1. The server returned a 5.1 type delivery status notification that clearly indicates the invalid address or domain.
    2. The server returned a standard know message that indicates that the address is invalid ("no such user", "user unknown", etc.)

Note that Dialog Insight also automatically manages non-standard error messages common to all major service providers (Hotmail, Yahoo, Sympatico, etc.).

Manual Error Management

Despite the constant evolution of rules governing how addresses are put on quarantine, multiple errors, considered to be permanent or hard bounces are not affected by these quarantine rules ("5xx" SMTP responses). These errors are grouped under two categories:

1. Errors due to an invalid address that are not detected
2. Various other errors, triggered by a variety of scenarios (messages rejected by anti-spam filter, full mailbox, etc.)

Dialog Insight constantly improves its automatic detection processes, but some situations might still require manual intervention using tools included in the application.

Feedback Loops

Another aspect that directly affects your reputation is the number of complaints that originate from the messages you send. The majority of service providers offer their users the ability to report a complaint by simply clicking on a “This is spam” option located right in their email interface; this type of complaint automatically compromises your reputation.

Fortunately, most of these service providers also use a protocol that gives the details of the complaints filed by their users. This process is commonly known as a "feedback loop" (FBL).

The FBL process is offered as a service by service providers, and lets you receive directly the complaints in an official format that can be read by a computer.

Dialog Insight offer a service that manages these complaints and also automatically applies a corrective measure upon reception of such a complaint, including the complete unsubscribing process of the contact and the addition of the related email address on your company's black list.

Subscription to FBL

Subscription to this service is done on an individual basis for each service provider. Dialog Insight has an agreement with the majority of providers and automatically receives replies to spam complaints filed against messages sent from their IP addresses.

The most important exception concerns Yahoo, who requires a specific subscription to their FBL process based on the domain name of the sender of the message, and who also requires a valid DKIM signature in each message.

Registering to Yahoo's FBL is done as part of the dedicated IP address configuration. For each domain name that you plan to use as the sender's email in your messages, you must ensure that there are relevant `postmaster@...` and `abuse@...` addresses and that you can receive these messages. A request will be sent to this address for each domain, and will include a link to confirm your request.

The remaining part of the process is automated and, from then on, all complaints done by the users of Yahoo will be directly sent to our servers.

Note : If messages are sent to Yahoo or Rogers addresses, you must subscribe to Yahoo's Feedback Loop. See Appendix 1.

Planning and Implementation

Phase 1 – Collection of Information

The following information will help Dialog Insight to plan your account setup accurately.

Assigned Addresses

What is the size of your contact list?

If you contact base is divided into multiple lists, indicate the number of distinctive contacts in total.

Complete the following table each type of communication you plan to send, how often you plan to do so and how many messages for each.

Type	Frequency	Volume

Example: Type = Newsletter, Frequency = Daily, Volume = 25,000

If possible, identify the "TOP 5" domains used in your contact list and the number of contacts for each of these domains. (If needed, Dialog Insight can establish this identification for you if you do not have the tools to perform it).

Domain	Number of contacts

Indicate the types of communications you are planning to send.

[ ] General communications / solicited promotion (bulletins, etc.)

[ ] Unsolicited communications (referrals, Tell-a-Friend, etc.)

[ ] Transactional communications (order follow-up, etc.)

Inventory of Domains

Provide the complete list of domains that will be used as sender addresses in your messages (From: ...@domain.com), for all contact lists and all communication types.

Important: For each of these domains, you must have access to the messages sent to the postmaster@domain.com address in order to register the related domain to the proper feedback loops.

Phase 2 – DNS configurations

Using the Phase 1 information, Dialog Insight will assign the necessary IP addresses and will send you a list of DNS entries to add to your domains.

Once these setups are completed and validated, you will be ready to send messages!

Appendix 1

Yahoo Feedback Loops (FeedbackLoop, FBL)

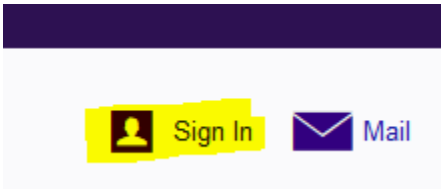
The person who requests this service must have a real-time access to messages sent to the postmaster of the domain for which the request is done (i.e. the domain of the sender's email address used in Dialog Insight messages).

Example: postmaster@yourdomain.com

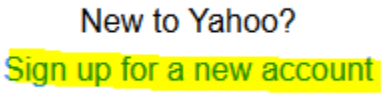
It is recommended to test sending the message to this address to make sure it is valid and that the message is received. As a matter of fact, although setting a postmaster address is required by most standards, not all domains apply this specification or know exactly where messages go.

Yahoo Account (YahooID)

The service request must be done from your Yahoo account. If you don't already have an account, you can create one by clicking on ***Sign In*** in the top right corner of Yahoo's website pages:



And then click on ***Sign up for a new account*** to fill out the new account request:

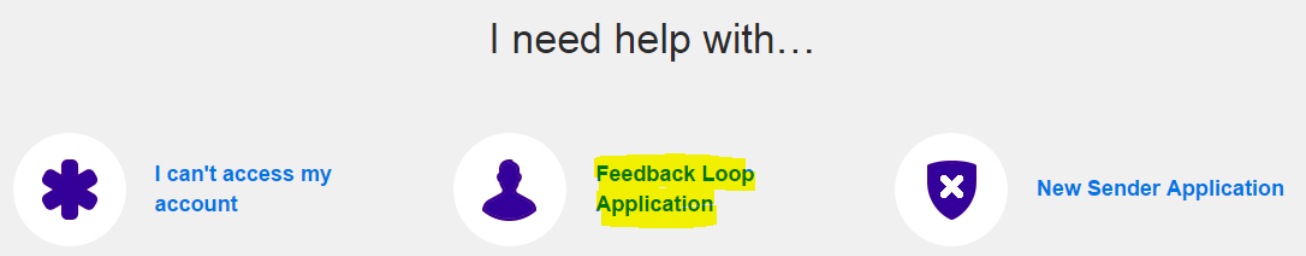


This is a standard account creation process, as found on most websites.

Request Form

The service request can be done at this page:
https://help.yahoo.com/kb/postmaster/

You then need to click on ***Feedback Loop Application***:



You must provide the following information:

- The client's general contact information
- The required information to select the reports to send (the ***Domain*** and ***Selector*** fields)
- The address to send the reports to

In addition to your contact information, you must also provide the following information:

- ***Reporting Email*** : yahoo@feedback.ofsys.com
- ***Selector*** : ofsys
- ***Request type*** : Add
- ***Domain*** : The name of the domain to register

The value for the ***Reporting EMail*** must always be yahoo@feedback.ofsys.com – this address is the general entry point in our application for any Yahoo spam emails.

The value for the ***Domain*** corresponds to the sender's email addresses used in messages sent using Dialog Insight. This is the domain for which we want spams to be reported. If you send messages from multiple domains (or multiple sub-domains of one main domain), you must submit a request form for each domain.

Finally, the value for the ***Selector*** identifies the applicable signatures – we do not only want to receive spam complaints from messages sent from Dialog Insight (we do not want to process other spam complaints). So, the ***Selector*** is the one selected by Dialog Insight when DNS entries for DKIM were created. We usually use "ofsys"

as the ***Selector***, which makes it easy for us to recognize our signatures. However, in some cases, the ***Selector*** could be different; in such a case, the appropriate value will be provided when your account is created.

Request Verification

Clicking on the ***Get Verification Code*** will send a message to postmaster@yourdomain.com

The code sent in this message needs to be entered on the page that follows. You must do this real-time, as you won't be able to come back later to enter the code. The message only includes the code and no link to access your request to complete it.

Once the provided code is entered, and the request submitted, your request should be processed within the next 48 hours.