BENEFITS OF USING SPF AND DKIM

How to increase deliverability and trustworthiness in email distribution from Questback when using custom sender address.
(i.e not using feedback@questback.net)

Updated on January 10th 2024 by Adnan Spahic.

Benefits of using SPF & DKIM

This document is intended for system administrators for the setup of the communication between Questback's mail server and the user's mail server when user want to have their own domain name as sender address to ensure higher deliverability and trustworthiness from the mail systems. (i.e. john.doe@company.com)

If you want to use custom sender address, please follow the instruction below. Please note that there is no guarantee that the emails aren't considered spam because of other reasons, like content-filtering.

Please forward this to the relevant persons or contact your local support for further instructions.

What is SPF?

SPF (Sender Policy Framework) is a DNS text entry which shows a list of servers that should be considered allowed to send mail for a specific domain. Incidentally the fact that SPF is a DNS entry can also consider a way to enforce the fact that the list is authoritative for the domain, since the owners/administrators are the only people allowed to add/change that main domain zone.

What is DKIM?

DKIM (DomainKeys Identified Mail) should instead be considered a method to verify that the messages' content is trustworthy, meaning that they weren't changed from the moment the message left the initial mail server. This additional layer of trust ability is achieved by an implementation of the standard public/private key signing process. Once again, the owners of the domain add a DNS entry with the public DKIM key which will be used by receivers to verify that the message DKIM signature is correct, while on the sender side the server will sign the entitled mail messages with the corresponding private key.

Should I as a customer of Questback use this?

SPF has become more popular as a way to ensure that incoming e-mail is received from a legitimate sender and DKIM are verifying that the messages' content is trustworthy. Many spam filters utilize this technique to stop spam. All Industry leading mail server products support SPF and DKIM.

By setting up a SPF and DKIM record in your domain and approving QuestBack IP's you will increase the deliverability of the email distributions and increase response rates for your Projects.

How can I do this for SPF?

Contact your IT department or domain administrators and ask them to configure SPF on your domain. Use this document as a guide to which IP addresses should be included.

A general SPF record looks like this:
Example Domain.com IN TXT "v=spf1 mx include:_spf.questback.net ~all "

This example will approve your domains mail servers and QuestBack IP addresses to allow sending of mail with your domain in the sender address.

Short explanation of the above record:
MX – Specifies that all mail servers that already have an MX record in your domain is approved.
INCLUDE – Includes SPF records from other domains, in this example _spf.questback.net contains all relevant IP-addresses that QuestBack sends from and will be kept updated by QuestBack with any new or changed IP-addresses.
~ALL – Means that emails from other servers should "SoftFail" (they will be accepted but marked).

The complete SPF Syntax can be found here:
http://www.openspf.org/SPF_Record_Syntax

How can i do this for DKIM?

You must specify a domain and a selector. The domain and the selector are not used in the generation of the public / private key pair. They will only be used to provide server and DNS setup instructions specific to you.

DomainKeys validate that the domain of the from address matches the domain that is sending the message. DomainKeys do not validate the domain of the return path. You must specify the domain that you will use in the from address (From: header) of your messages. (If you will be sending out mail from multiple domains, you will need to go through this process for each one.)

A single domain can use more than one set of DomainKeys. You must specify a selector which will be used to specify (or "select") the set of DomainKeys you will be using to sign your messages. If you are only going to use one set of DomainKeys, it does not matter what you enter, and you can use something like "key1".

To set up a DKIM Key pair, please request that at QuestBack Support. We will generate the private and public keys and keep the private key safe on our server.

The public key will be sent to you with some instructions for setting it up as a TXT record for the sending domain.

The key is generated from:
https://www.socketlabs.com/domainkey-dkim-generation-wizard/

HOW CAN I DO THIS FOR DOMAIN?

Your e-mail gateway does not allow internal addresses (yourdomain.com) sent from outside servers (questback.net) into your system.

All of these domains and IP's might be used for outgoing email:
* mail1.questback.com - 141.147.10.7
* mail2.questback.com - 132.226.204.117
* mail3.questback.com - 129.159.250.38
* mail4.questback.com - 193.122.53.174
* mail5.questback.com - 129.159.252.119

How to verify that everything is set up correctly?

To check if everything is set up correctly, use - https://www.mail-tester.com/ - and send an invitation to the given e-mail address from Questback Essentials with your custom sender address.

Recommended reading

Since this is just a brief document describing the most common way to use SPF & DKIM to approve QuestBack servers to send with your domain, we recommend anyone implementing SPF to read the following articles, since your mail server infrastructure might have additional needs.

http://en.wikipedia.org/wiki/Sender_Policy_Framework
http://www.openspf.org/SPF_Record_Syntax
https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail