WorldAPP

RECOMMENDATIONS
For Mail Domains

WEB: www.worldapp.com • www.keysurvey.com
E-MAIL: info@worldapp.com

US: +1(781)-849-8118
US TOLL FREE: +1(888)-708-8118
UK: +44(0)-8451-303345
AU: +1(800)-554-985
FR: +33(0)1-7890-05-45
SG: +65-673-318-35

WorldAPP

RECOMMENDATIONS FOR MAIL DOMAINS

Last updated on 12 January 2016

Target audience

These recommendations of setting up Email Domains should be applied if, while sending emails from your application hosted by WorldAPP, you are using an address other than @keysurvey.com (or @ your branded site) or in case email from your application doesn't reach the recipients in your domain.

Technical recommendations

The number of companies using security software is growing rapidly. This software is aimed at protection from replacement of the sender's e-mail address (spoofing), such as Sender Policy Framework (SPF, analogy of Microsoft Sender ID), DomainKeys Identified Mail (DKIM).

Further information on these technologies can be found here:

SPF: http://www.openspf.org

Sender ID: http://www.microsoft.com/senderid

DKIM: http://www.dkim.org

Our suggestion is to extend the use of these technologies, if you're using this type of software, for your domain taking into consideration that emails, containing the signature of your domain, will be sent from WorldAPP servers. The settings that need to be applied in order to have mail accepted as legitimate by SPF and DKIM, that was sent from the WorldAPP server and containing your domain name, are described below. The above mentioned suggestion refers not only to launches going to addresses @ your company domain, but also to other domains (Hotmail, Yahoo, Gmail, AOL, etc.)

Sender Policy Framework (SPF) Configuration

Utilizing Sender Policy Framework (SPF) records is strongly recommended by WorldAPP, it is greatly decreases the risk in which emails launched from our system will be considered as a phishing attempt or spam. This is accomplished by including the address of our mail servers to your DNS records hosted by your domain register. If you are unable to make the provided changes, you will still be able to send emails from within our platform, but with the potential of reduced success in delivery. In our experience, users typically provide the following instructions to their IT department in order perform these changes.

- Sign in to your DNS hosting provider's website.
- Select your domain.
- Locate the page where you can edit DNS records for your domain.
    - If setting up a SPF record for the first time, please create a new TXT record with the following value: **v=spf1 include:spf1.worldapp.com ~all**
    - If a SPF record already exists, please update it with the additional parameter **include:spf1.worldapp.com.**

An example of a SPF record with multiple parameters would appear similar to: **v=spf1 mx:google.com include:spf.protection.outlook.com include:spf1.worldapp.com ~all**

- Using any DNS lookup service (such as http://mxtoolbox.com/TXTLookup.aspx) check to ensure the settings are in place. This is done by specifying your domain and selecting the TXT lookup option.
    - For instance, checking the TXT record for your.domain.com produces the following result:

Type	Domain Name	TTL	Record
TXT	your.domain.com	15min	v=spf1 include:spf1.worldapp.com ~all

Here you will see an example where a new TXT was created, where spf1.worldapp.com ~all was the only value entered. Your individual result may vary, if you are using multiple third-party services to send email. However, include:spf1.worldapp.com should be still specified somewhere within the record shown.

For additional technical information regarding the Sender Policy Framework, please visit http://www.openspf.org/SPF_Record_Syntax.

DomainKeys Identified Mail (DKIM) Configuration

Much like using SPF records, the use of DomainKeys Identified Mail (DKIM) will improve the delivery of messages by providing the recipient of the email the ability to verify that the domain signature has come from your domain, and has not been modified along the way.

- Sign in to your DNS hosting provider's website.
- Select your domain.
- Locate the page where you can edit DNS records for your domain.
    - Please add a TXT record for the ks-mass._domainkey sub-domain of your primary domain that contains the information from the TXT record of **ks-mass._domainkey.worldapp.com**.

If you were to check the domain **ks-mass._domainkey.worldapp.com** using a DNS lookup service (such as http://mxtoolbox.com/TXTLookup.aspx), you will see only 1 TXT record with the following value:

k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDRugQcd2luaomuzGa5xZGPHjrLsbSc/YxnECw/b0iX6KySHKU/H4dRzUBJtdsEkqZYp9OEIzhpj2ndIjK0qXpyeST5ZriB2ZKNkgNI7Ld+vRcUveL21JW+fAv35SChmYhD6bsAYduwDVfyB61p78sGJ0csAiyngySI+uoHRkTfowIDAQAB

Please **copy** this value and use it as TXT value for domain you wish to use in your **from** address. For instance, if the domain you wish to use is "@customer-survey.com" you will want to create the following sub-domain: **ks-mass._domainkey.customer-survey.com** as this will be the domain used by mail system for the key verification.

Once this is complete, please contact WorldAPP support so that our technical teams can process the final steps of the verification from our side. Once confirmed by our team, the process will be complete.

Whitelisting

If it turns out impossible to apply the changes described above, then in order to prevent rejection of emails from your application, it is necessary to provide access to your mail server for emails coming from the following IPs of WorldAPP servers: **216.34.99.11** through **216.34.99.19**