SALESmanago

New Gmail and Yahoo requirements

Configure SPF, DKIM, and DMARC with SALESmanago

Contents

1. Why do you need to implement the SPF, DKIM, and DMARC protocols?

Starting from 1 February 2024, Gmail and Yahoo introduced stricter authentication requirements for senders of mass mailings (i.e., those who have ever sent more than 5,000 emails in one day). The new requirements are designed to protect email users from spam, phishing, and malware. This means that the three email authentication protocols that have so far been strongly recommended—SPF, DKIM, and DMARC—are now becoming obligatory (otherwise, these email clients may block your mailings to @gmail and @yahoo addresses).

These three protocols serve the following purposes:

- **SPF (Sender Policy Framework):** Specifies the servers and domains that are authorized to send email on behalf of your organization.
- **DKIM (DomainKeys Identified Mail):** Adds a digital signature to every outgoing message, which lets receiving servers verify the message actually came from your organization.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Lets you tell receiving servers what to do with outgoing messages from your organization that don't pass SPF or DKIM.

Source: Google Help Center (https://support.google.com/a/answer/2466580?hl=en)

The new requirements are likely to apply to all SALESmanago customers who:

- use a SALESmanago Email Marketing sender account, or
- use an External (SMTP) sender account and send (regularly or occasionally) more than 5,000 emails a day.

If you don't know how to implement these protocols, read the instructions and explanations provided below.

NOTE: Start by implementing the SPF and DKIM protocols and only then proceed to the DMARC protocol. Without SPF and DKIM, DMARC will not work correctly.

2. Implementing email authentication protocols for your domain

The SPF, DKIM, and DMARC protocols are usually implemented in the **DNS (Domain Name System) settings** for your domain. Most likely, you will be able to implement all these protocols from a single place, by adding four different records to your domain's settings.

Additionally, **we recommend adding a fifth record that will enable SALESmanago to automatically verify your DKIM configuration**, saving you time and effort.

NOTE: The instructions below are of a generic nature. The actual process may look different depending on the eCommerce platform, domain registrar, hosting provider, or CDN provider whose services you use.

Step 1. Determine where you can edit your DNS settings.

Depending on the way in which your website is set up, consider these three possibilities:

A. **E-store set up on a SaaS eCommerce platform** (such as Shopify or BigCommerce): Log into your e-store account and search for DNS settings. For instance, on Shopify, you need to go to Settings → Domains → Domain settings → Edit DNS settings.

B. **Domain purchased via a hosting provider** (such as OVH or A2 Hosting): Log into your hosting account and go to the control panel (which can be called "user panel", "domain configuration panel", etc).

C. **Domain purchased via a domain registrar** (such as GoDaddy or OVH): Log into your domain account and go to the control panel (which can be called "user panel", "domain configuration panel", etc).

D. **Website served via a Content Delivery Network—CDN** (such as Cloudflare): Log into your CDN account and go to the control panel (which can be called "user panel", "domain configuration panel", etc).
In Cloudflare, go to DNS → Records:
https://developers.cloudflare.com/dns/manage-dns-records/how-to/create-dns-records/

NOTE: If you have more than one domain, make sure to select the one you want to configure.

Step 2. Find the right place in the DNS settings.

After logging into the account that allows you to edit your DNS settings, look for the place where you can **add records for your domain**. This place (section, tab, etc.) can be called, for instance, *DNS Settings*, *Zone Editor*, *DNS Management*, *Name Server Configuration*, or *DNS Record Management*.

It is possible that you will see buttons like *Add TXT record* and *Add CNAME record*; or you may need to click a button for adding a record and then select the record type from a list. If you can’t find the option to add a record for your domain, consult the help materials of your service provider (eCommerce platform, domain registrar, hosting provider, or CDN provider) or contact their customer support.

Step 3. Add records for the email authentication protocols.

To implement all three protocols required, you will need to add **four records** of the following types:

Protocol	Record type
SPF	TXT
DKIM	CNAME **(x2)**
DMARC	TXT

You will need to configure each of these records by providing the following values:

A. Host (*Host record*, *Host name*, *Name*, *Domain*, etc.),
B. Text value (*Main value*, *Record*, *Value*, *Content*, etc.), and
C. TTL (Time to Live).

Additionally, we recommend adding **a fifth record that will enable SALESmanago to automatically verify your DKIM configuration**, saving you time and effort (see Step 3.3).

TIPS:

- After completing the *Host* field, you may see that a dot (full stop) was added at its end. Don't try to delete it—this is a required formatting element.
- If you are in doubt which field is the *Host* field, look at your existing records and check which field contains domain addresses.

Read the instructions below to find out how you should complete the different input fields when defining the new records.

NOTE: Before implementing any of the protocols, make sure that you don't have them in place already. You will probably be able to check this in the same control/user/configuration panel where you can add a new record – simply review the list of existing records.

Note that the SPF record may need updating – see the instructions below.

Step 3.1. Adding the SPF protocol

Add a **TXT record** for your domain.

You will probably see a number of input fields that allow you to define the new record. Pay attention to these three fields:

A. Host (*Host record*, *Host name*, *Name*, *Domain*, etc.):

In this field, enter the name of your domain accompanied by the top-level domain, e.g.:

yourcompany.com, *yourstore.de*, *yourecommerce.es*

B. Text value (*Main value*, *Record*, *Value*, *Content*, etc.):

In this field, enter the following value:

```
v=spf1 include:_spf.jupiter.salesmanago.pl
```

NOTE: If you already have an existing `v=spf1` record, simply extend it by adding:

```
 include:_spf.jupiter.salesmanago.pl
```

For instance, if your current entry is:

```
v=spf1 mx include: _spf.google.com -all
```

Change it to:

```
v=spf1 mx include: _spf.google.com
include:_spf.jupiter.salesmanago.pl -all
```

Note that flags, such as `-all`, should be placed after the newly added part.

C. TTL (Time to Live):

The TTL (Time to Live) should be set to 1 hour (3600 seconds).

Add the ready record by clicking *Save*, *OK*, *Done*, etc. You don’t need to take any additional steps on the SALESmanago platform. You can now proceed to the configuration of DKIM.

IMPORTANT: The SPF protocol will be implemented for your domain within several hours, but **it can take up to 24 hours for the changes to become visible in your domain settings** (due to a DNS propagation delay).

Step 3.2. Adding the DKIM protocol

Add **two CNAME records** for your domain. You will probably see a number of input fields that allow you to define the new records. Pay attention to the three fields described below.

CNAME RECORD 1:

A. Host (*Host record*, *Host name*, *Name*, *Domain*, etc.):

In this field, enter the following value:

```
salesmanago._domainkey.example.com
```

replacing the fragment highlighted in green with your own details.

EXAMPLES:

```
salesmanago._domainkey.yourcompany.com
salesmanago._domainkey.yourstore.de
salesmanago._domainkey.yourecommerce.es
```

B. Text value (*Main value*, *Record*, *Value*, *Content*, etc.):

In this field, enter the following value:

`salesmanago._domainkey.smgrid.com`

C. TTL (Time to Live):

The TTL (Time to Live) should be set to 1 hour (3600 seconds).

Add the ready record by clicking *Save*, *OK*, *Done*, etc. Next, **add the second CNAME record** described below.

CNAME RECORD 2:

A. Host (*Host record*, *Host name*, *Name*, *Domain*, etc.):

In this field, enter the following value:

```
salesmanago2._domainkey.example.com
```

replacing the fragment highlighted in green with your own details:

EXAMPLES:

`salesmanago2._domainkey.`*yourcompany.com*
`salesmanago2._domainkey.`*yourstore.de*
`salesmanago2._domainkey.`*yourecommerce.es*

B. Text value (*Main value*, *Record*, *Value*, *Content*, etc.):

In this field, enter the following value:

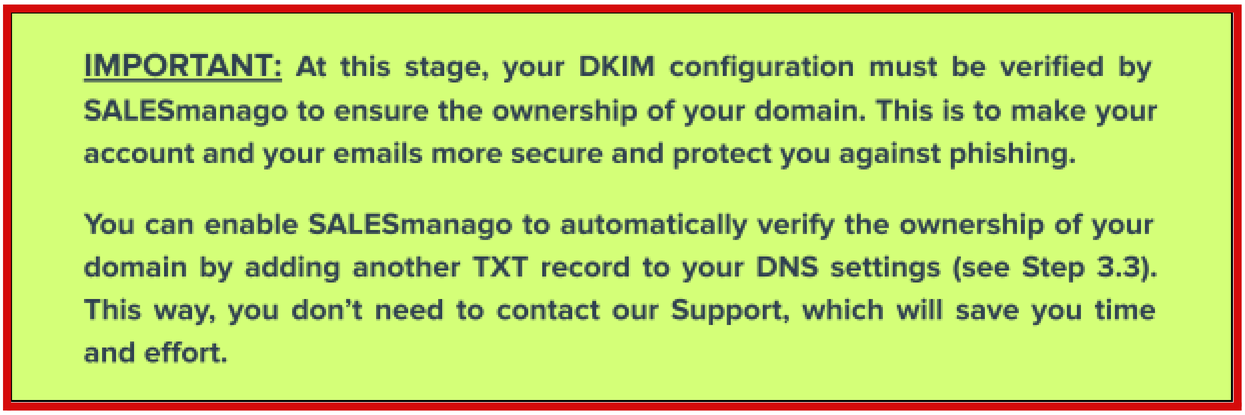
`salesmanago2._domainkey.smgrid.com`

C. TTL (Time to Live):

The TTL (Time to Live) should be set to 1 hour (3600 seconds).

Add the ready record by clicking *Save*, *OK*, *Done*, etc.

IMPORTANT: The DKIM protocol will be implemented for your domain within several hours, but **it can take up to 24 hours for the changes to become visible in your domain settings** (due to a DNS propagation delay).



IMPORTANT: At this stage, your DKIM configuration must be verified by SALESmanago to ensure the ownership of your domain. This is to make your account and your emails more secure and protect you against phishing.

You can enable SALESmanago to automatically verify the ownership of your domain by adding another TXT record to your DNS settings (see Step 3.3). This way, you don't need to contact our Support, which will save you time and effort.

Step 3.3. Automate DKIM verification by SALESmanago by adding a dedicated TXT record (optional)

Following the implementation of the DKIM protocol (through the addition of the two CNAME records described above), the ownership of your domain must be verified by SALESmanago. The purpose of this requirement is to make your account and your emails more secure, and to protect you against phishing.

The ownership of your domain can be confirmed automatically if you add another TXT record for your domain. This is the recommended option because it will accelerate the verification process, saving you time and effort.

Otherwise, please contact us at support@salesmanago.com as soon as you implement your DKIM protocol, and ask to have the ownership of your domain confirmed by our specialists.

If you want to use the automatized option, **add another TXT record for your domain** and fill its fields as follows:

A. **Host (*Host record*, *Host name*, *Name*, *Domain*, etc.):**

In this field, enter the name of your domain accompanied by the top-level domain, e.g.:

yourcompany.com, *yourstore.de*, *yourecommerce.es*

B. **Text value (*Main value*, *Record*, *Value*, *Content*, etc.):**

In this field, enter the following value:

```
smv=clientId
```

replacing the fragment highlighted in green with your own Client ID.

You can find your Client ID on the SALESmanago platform, by navigating to **Menu → Integration Center → API → API v2 tab**.

C. **TTL (Time to Live):**

The TTL (Time to Live) should be set to 1 hour (3600 seconds).

Add the ready record by clicking *Save*, *OK*, *Done*, etc. Now, the ownership of your domain will be verified by SALESmanago automatically. At this stage, you can proceed to configuring the DMARC protocol.

Step 3.4. Adding the DMARC protocol

> **NOTE: Before implementing the DMARC protocol, make sure that you have the SPF and DKIM protocols implemented. You will probably be able to check this in the same control/user/configuration panel.**
>
> **Without these protocols, DMARC will fail to work correctly.**
>
> **Also, make sure that you have had your DKIM protocol verified by SALESmanago (to confirm the ownership of your domain and increase your security). The recommended option is to automate the verification by adding another, simple TXT record to your DNS settings – see Step 3.3.**

Add a **TXT record** for your domain.

You will probably see a number of input fields that allow you to define the new record. Pay attention to these three fields:

A. Host (*Host record*, *Host name*, *Name*, *Domain*, etc.):

In this field, enter the following value:

```
_dmarc.example.com
```

replacing the fragment highlighted in green with your own email sending domain.

EXAMPLES:

```
_dmarc.yourcompany.com

_dmarc.yourstore.de

_dmarc.yourecommerce.es
```

B. **Text value (*Main value*, *Record*, *Value*, *Content*, etc.):**

In this field, enter your DMARC record. If you are unsure which parameters and values you should use for your DMARC record, consider using the format recommended by SALESmanago.

RECOMMENDED DMARC VALUE

```
v=DMARC1; p=quarantine;
rua=mailto:youremailaddress@example.com;
ruf=mailto:failureemailaddress@example.com; adkim=r; aspf=r;
```

Copy this formula and paste it into the main input field of the new TXT record, replacing the details highlighted in green with your own data:

- The **rua** parameter is the address at which you will receive aggregate reports on your email traffic.
- **Ruf** is the address at which you will receive reports on failed authentication checks. Note that this parameter is not supported by Gmail.

EXAMPLES:

```
v=DMARC1; p=quarantine; rua=mailto:emailmanager@company.com;
ruf=mailto:emailfailures@company.com; adkim=r; aspf=r;
```

```
v=DMARC1; p=quarantine; rua=mailto:administrator@yourcompany.de;
ruf=mailto:dmarcfailures@yourcompany.de; adkim=r; aspf=r;
```

You can also customize individual values based on the parameters (tags) and definitions set out in the table provided in the Appendix.

NOTE: We recommend including the following tags: aspf=r; adkim=r; in the record formula. Otherwise, if you set your policy to anything different than p=none, your messages will not be delivered at all.

C. **TTL (Time to Live):**

The TTL (Time to Live) should be set to 1 hour (3600 seconds).

Add the ready record by clicking *Save*, *OK*, *Done*, etc. You don't need to take any additional steps on the SALESmanago platform.

IMPORTANT: The DMARC protocol will be implemented for your domain within several hours, but **it can take up to 24 hours for the changes to become visible in your domain settings** (due to a DNS propagation delay).

If you have any questions or doubts concerning the configuration of your email authentication protocols, or if you would like to have your setup verified by our Support specialist, please contact us at:

support@salesmanago.com

3. Quick summary

The table below sums up the DNS entries required by the new Gmail and Yahoo policies. Review its contents and compare them with your new records.

Remember that the details marked in green are just placeholders and must be replaced with your own data.

Protocol	Name	Type	Value	TTL
SPF	example.com	TXT	v=spf1 include:_spf.jupiter.salesmanago.pl	3600
DKIM	salesmanago._domainkey.example.com	CNAME	salesmanago._domainkey.smgrid.com	3600
	salesmanago2._domainkey.example.com	CNAME	salesmanago2._domainkey.smgrid.com	3600
DMARC	_dmarc.example.com	TXT	v=DMARC1; p=quarantine; rua=mailto:dmarcreports@example.com; ruf=mailto:dmarcreports@example.com; adkim=r; aspf=r;	3600

NOTE: If you have an existing `v=spf1` record, simply extend it by adding:

```
include:_spf.jupiter.salesmanago.pl
```

Note that flags, such as -all, should be placed after the newly added part. You can read more in Step 3.1.

Additionally, we encourage you to **add another TXT record** that will enable SALESmanago to automatically verify the ownership of your domain. This way, you won't need to contact our Support after implementing DKIM. See **Step 3.3** for more information.

Record	Name	Type	Value	TTL
Automatic DKIM verification by SALESmanago	example.com	TXT	smv=clientId	3600

APPENDIX: DMARC record elements

The table below presents parameters (tags) and values for DMARC records, as described by Google:

https://support.google.com/a/answer/10032169?sjid=14098442164638657890-EU#zippy=%2Cdmarc-record-tag-definitions-and-values

The table describes the different elements of a DMARC record and sets out the different configuration options you have.

If you are unsure which values you should use for your DMARC record, consider using the recommended SALESmanago format (see Section 3.3 above).

Tag	Description and values
v	DMARC version. Must be DMARC1. **This tag is required.**
p	Instructs the receiving mail server what to do with messages that don't pass authentication. **none**—Take no action on the message and deliver it to the intended recipient. Log messages in a daily report. The report is sent to the email address specified with the rua option in the record. **quarantine**—Mark the messages as spam and send it to the recipient's spam folder. Recipients can review spam messages to identify legitimate messages. **reject**—Reject the message. With this option, the receiving server usually sends a bounce message to the sending server. **This tag is required.** BIMI note: If your domain uses BIMI, the DMARC p option must be set to quarantine or reject. BIMI doesn't support DMARC policies with the p option set to none.

pct	Specifies the percent of unauthenticated messages that are subject to the DMARC policy. When you gradually deploy DMARC, you might start with a small percentage of your messages. As more messages from your domain pass authentication with receiving servers, update your record with a higher percentage, until you reach 100 percent. Must be a whole number from 1 to 100. If you don't use this option in the record, your DMARC policy applies to 100% of messages sent from your domain. **This tag is optional.** BIMI note: If your domain uses BIMI, your DMARC policy must have a pct value of 100. BIMI doesn't support DMARC policies with the pct value set to less than 100.
rua	Email address to receive reports about DMARC activity for your domain. The email address must include mailto: For example: mailto:dmarc-reports@solarmora.com To send DMARC reports to multiple emails, separate each email address with a comma and add the mailto: prefix before each address. For example: mailto:dmarc-reports@solarmora.com, mailto:dmarc-admin@solarmora.com This option can potentially result in a high volume of report emails. We don't recommend using your own email address. Instead, consider using a dedicated mailbox, a group, or a third-party service that specializes in DMARC reports. **This tag is optional.**
ruf	Not supported. Gmail doesn't support the ruf tag, which is used to send failure reports. Failure reports are also called forensic reports.

sp	Sets the policy for messages from subdomains of your primary domain. Use this option if you want to use a different DMARC policy for your subdomains. **none**—Take no action on the message and deliver it to the intended recipient. Log messages in a daily report. The report is sent to the email address specified with the rua option in the policy. **quarantine**—Mark the messages as spam and send it to the recipient's spam folder. Recipients can review spam messages to identify legitimate messages. **reject**—Reject the message. With this option, the receiving server should send a bounce message to the sending server If you don't use this option in the record, subdomains inherit the DMARC policy set for the parent domain. **This tag is optional.**
adkim	Sets the alignment policy for DKIM, which defines how strictly message information must match DKIM signatures. (...) **s**—Strict alignment. The sender domain name must exactly match the corresponding d=*domainname* in the DKIM mail headers. **r**—Relaxed alignment (default). Allows partial matches. Any valid subdomain of d=*domain* in the DKIM mail headers is accepted. **This tag is optional.**
aspf	Sets the alignment policy for SPF, which specifies how strictly message information must match SPF signatures. (...) **s**—Strict alignment. The message From: header must exactly match the domain name in the SMTP MAIL FROM command **r**—Relaxed alignment (default). Allows partial matches. Any valid subdomain of domain name is accepted. **This tag is optional.**

Source: Google Help Center
https://support.google.com/a/answer/10032169?sjid=14098442164638657890-EU#zippy=%2Cdmarc-record-tag-definitions-and-values