SALESmanago

Email sending requirements

Configure DNS records with SALESmanago

Contents

1. Rationale

1.1. Why do I need to implement the SPF, DKIM, and DMARC records?

Starting from 1 February 2024, Gmail and Yahoo introduced stricter authentication requirements for senders of mass mailings. 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)

In light of the new policies, SALESmanago now requires these three protocols for new sender accounts. **Starting in late September 2025, these protocols will be mandatory for all sender accounts.**

If you don't know how to implement the required DNS records, read the instructions and explanations provided below. If you have experience in configuring domain settings, you can go directly to Section 3: *Quick summary*.

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.

1.2. Why should I implement the MX record?

An MX record tells email servers where to deliver incoming emails. While MX records are generally used for incoming mail, they also serve as an important indicator of a domain's credibility and authenticity.

More and more email servers are paying attention to the verification of the sender's domain, and the MX record is now required by an increasing number of email clients. Based on our research and industry best practices, we recommend implementing this record – for both sending and reply-to domains.

Your reply-to domain probably already has an MX record. Be sure to confirm this. The sending domain, in turn, may require adding this record.

If you don't know how to implement an MX record, read the instructions and explanations provided below. If you have experience in configuring domain settings, you can go directly to Section 3: *Quick summary*.

2. Implementing DNS records for your domain

All the required and recommended records—SPF, DKIM, DMARC, and MX—are usually implemented in the **DNS (Domain Name System) settings** for your domain. Most likely, you will be able to implement all these records from a single place.

Additionally, **we recommend adding a dedicated 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 the DNS records.

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

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

You 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.)
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). Also, consider implementing the **recommended MX record** (see Step 3.5).

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. If you have experience in managing DNS records, you can go directly to Chapter 3 for a one-page summary.

IMPORTANT

- Before implementing any of the protocols, **make sure 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).

- Implement SPF and DKIM **before** implementing DMARC.

Step 3.1. Adding the SPF record

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 should be set to 1 hour (3600 seconds).

Add the 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 configuring DKIM.

IMPORTANT: The SPF record 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 records

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 part 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 should be set to 1 hour (3600 seconds).

Add the 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 part 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 should be set to 1 hour (3600 seconds).

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

IMPORTANT: The DKIM record 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 confirm the ownership of your domain. The purpose 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. Automating DKIM verification by SALESmanago by adding a dedicated TXT record

Following the implementation of the DKIM record (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.

To enable the automatic confirmation of domain ownership, add another TXT record for your domain and complete 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 part 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 should be set to 1 hour (3600 seconds).

Add the 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 record.

IMPORTANT: If for some reason you are unable to implement this TXT record, please contact us at support@salesmanago.com as soon as you implement your DKIM record and ask to have the ownership of your domain confirmed by our specialists.

Step 3.4. Adding the DMARC record

NOTE: Before implementing the DMARC record, make sure you have the SPF and DKIM records implemented. You will probably be able to check this in the same control/user/configuration panel.

Without these records, DMARC will fail to work correctly.

Also, make sure that your DKIM records have been verified by SALESmanago (to confirm domain ownership). The recommended option is to automate the verification by adding another, simple TXT record to your DNS settings – see Step 3.3 above.

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 part 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, define your DMARC settings. If you are unsure which parameters and values to use, consider implementing 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 the settings 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 should be set to 1 hour (3600 seconds).

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

IMPORTANT: The DMARC record 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 3.5. Adding the MX record

The MX record should be configured for **both your reply-to domain and your sending domain.**

Your reply-to domain probably already has an existing MX record (otherwise, it wouldn't receive incoming mail). Be sure to confirm this by reviewing the list of existing DNS records for this domain.

- If you find a record of type "MX" in the list, no changes are needed for this domain.
- If there is no MX record on your reply-to domain yet, add one by following the instructions on page 16.

When you are certain that your reply-to domain has an MX record, proceed to configure the settings for your sending domain.

For the sending domain, the course of action depends on whether you use the same domain for both sending and receiving emails.

- If the answer is **yes**, no additional action is required—it is sufficient to have one MX record on your domain.

  EXAMPLE: You use the following email addresses:

  Sender email address: *newsletter@company.com*

  Reply-to email address: *contact@company.com*

  Since both addresses use the same domain (*company.com*), a single MX record is enough.

- If the answer is **no**, i.e., if you use **different domains or subdomains** for sending and receiving mail, you need to implement a separate MX record for the sending domain.

  EXAMPLE: You use the following email addresses:

  Sender email address: *company@newsletter.company.com*

  Reply-to email address: *contact@company.com*

  In this case, you need two MX records: one for the *newsletter.company.com* subdomain and one for the *company.com* domain.

Implementing an MX record

If any of your domains does not have an MX record, edit its DNS settings and **add a record of type "MX"**.

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:

```
10 mail.example.com
```

replacing the parts highlighted in green with your preferred **priority** and your **mail server name** (which includes the name of your domain accompanied by the top-level domain).

EXAMPLES:

0 yourserver.yourcompany.com

10 emailserver.youre-store.de

20 mailserver.yourecommerce.es

The **priority** is a numeric value that determines the order in which mail servers are used. The lower the number, the higher the priority. If multiple MX records are defined for a single domain, mail is delivered to the server with the lowest priority number first. If two MX records have the same priority, mail is distributed randomly between them.

The priority must be a whole number (integer). The minimum value is 0 (highest priority) and the maximum value is typically 65,535.

If you have no MX record yet, you can enter 10 as the priority number.

Continued on the next page...

The choice of the **mail server** that will handle incoming messages depends on your internal arrangements. If you already have an MX record on your reply-to domain and you don't know what server name to enter when configuring this record on the sending domain, you can look up the value of that first (already existing) MX record and copy the server name from there.

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

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

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

IMPORTANT: The MX record 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 DNS records, 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 or recommended by SALESmanago. 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.

DNS Record	Host (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
Automatic DKIM verification by SALESmanago	example.com	TXT	smv=clientId	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
MX	example.com	MX	10 mail.example.com	3600

NOTE: If you already have a `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 (see Step 3.1).

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 to apply 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