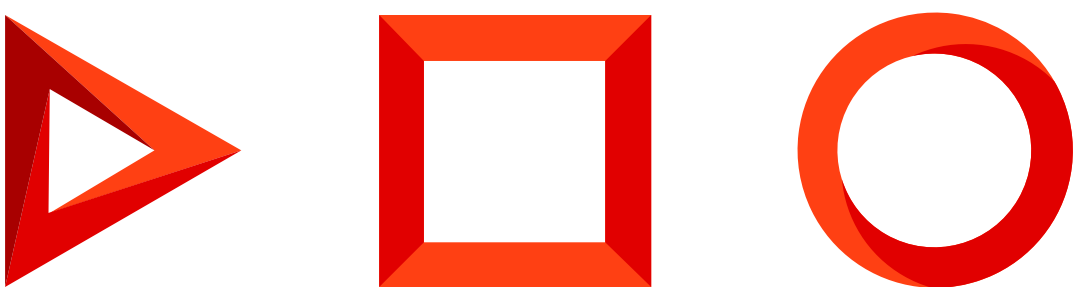
Creatio Academy

# Email domain verification

Version 7.17



# Table of Contents

# Domain verification for the Elastic Email provider

PRODUCTS: MARKETING

If you plan to send emails using the Elastic Email provider in Creatio, verify your email address and the corporate domain.

In this case, your recipients who use MS Outlook, Hotmail, Gmail and other common mailing services, will see that an email was sent from your provider's server on your behalf (this information is available in the “From” field). For example, if you are sending emails via Elastic Email, the “From” field of the emails may contain the following text: “Creatio <info@creatio.com> via elasticemail.com”.

To verify your email addresses and domain, perform the following steps:

1. Add your corporate domain on the [ *Bulk email settings* ] page. Read more >>>
2. Obtain SPF and DKIM records. Read more >>>
3. Specify SPF and DKIM records in the DNS area of your domain Read more >>>

**Attention.** If your domain is unverified, Elastic Email limits your daily number of emails to 50.

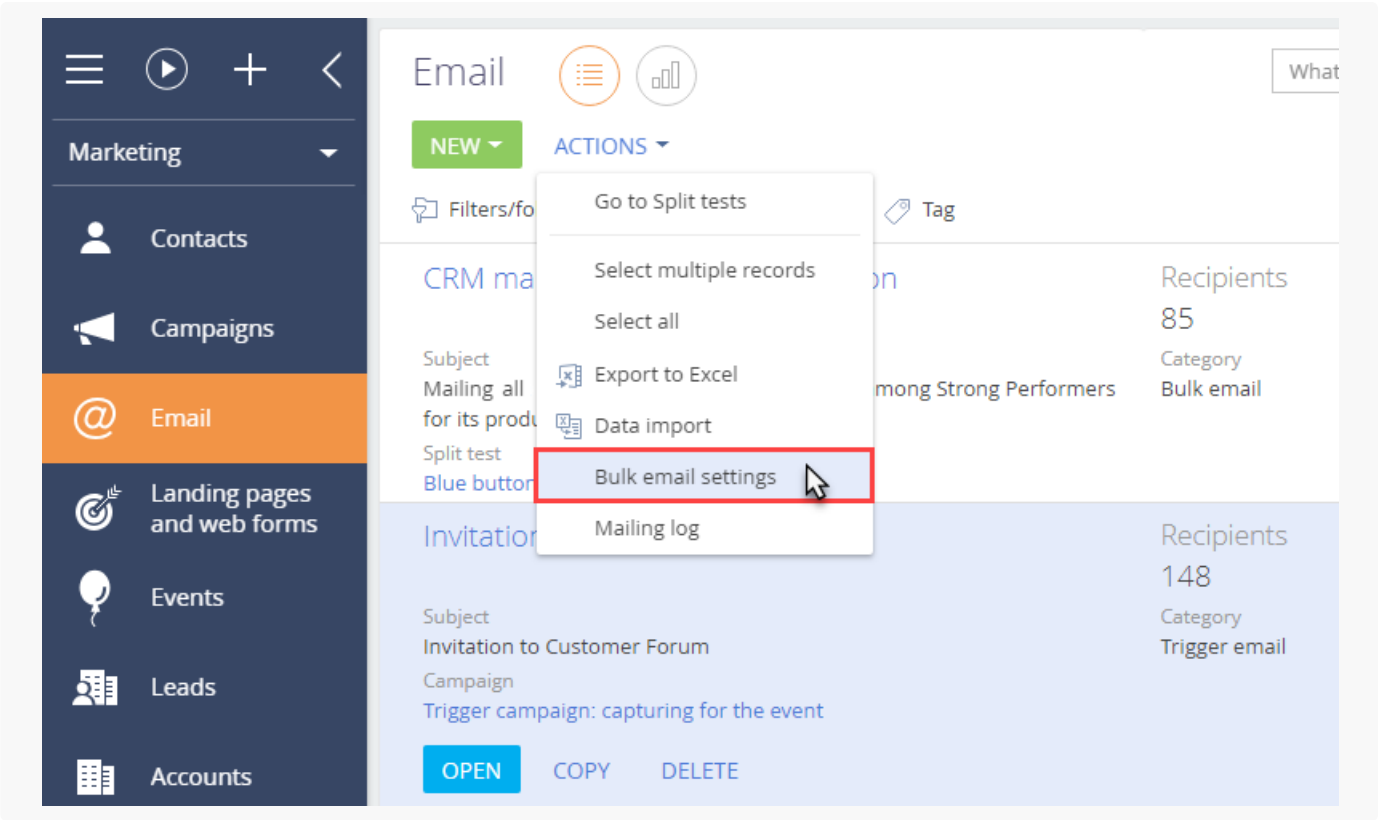
**Note.** Only custom email domains can be verified. Public domains (for example, gmail.com, yahoo.com, etc.) cannot be verified. We do not recommend using public domains for bulk emails. Such emails have a high risk of being marked as spam and ruining the reputation of the sender IP address.

## Add corporate domain on the [ *Bulk email settings* ] page

To start sending the emails, perform the following settings:

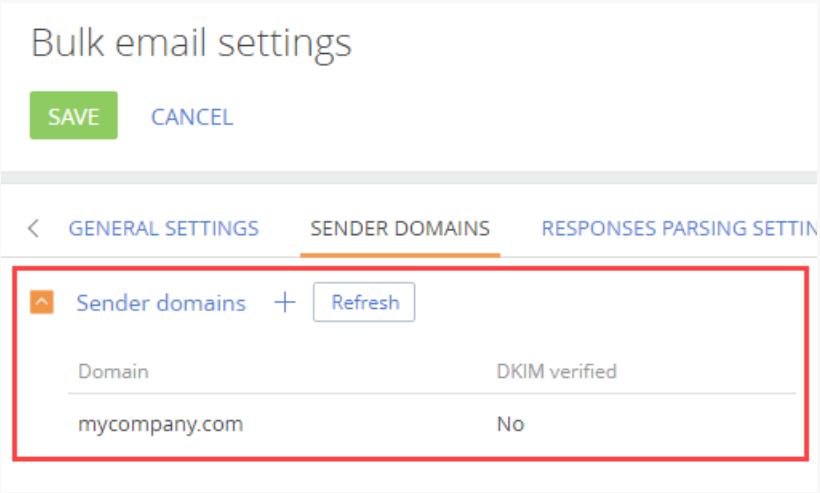
1. In the [ *Email* ] section, select **Email settings** in the [ *Actions* ] menu (Fig. 1)

Fig. 1 Opening the email settings page




2. On the [ *Email settings* ] page, specify the domain of the necessary email address in the **Sender domain** area, i.e., “mycompany.com” (Fig. 2).

Fig. 2 The [ *Sender domains* ] area



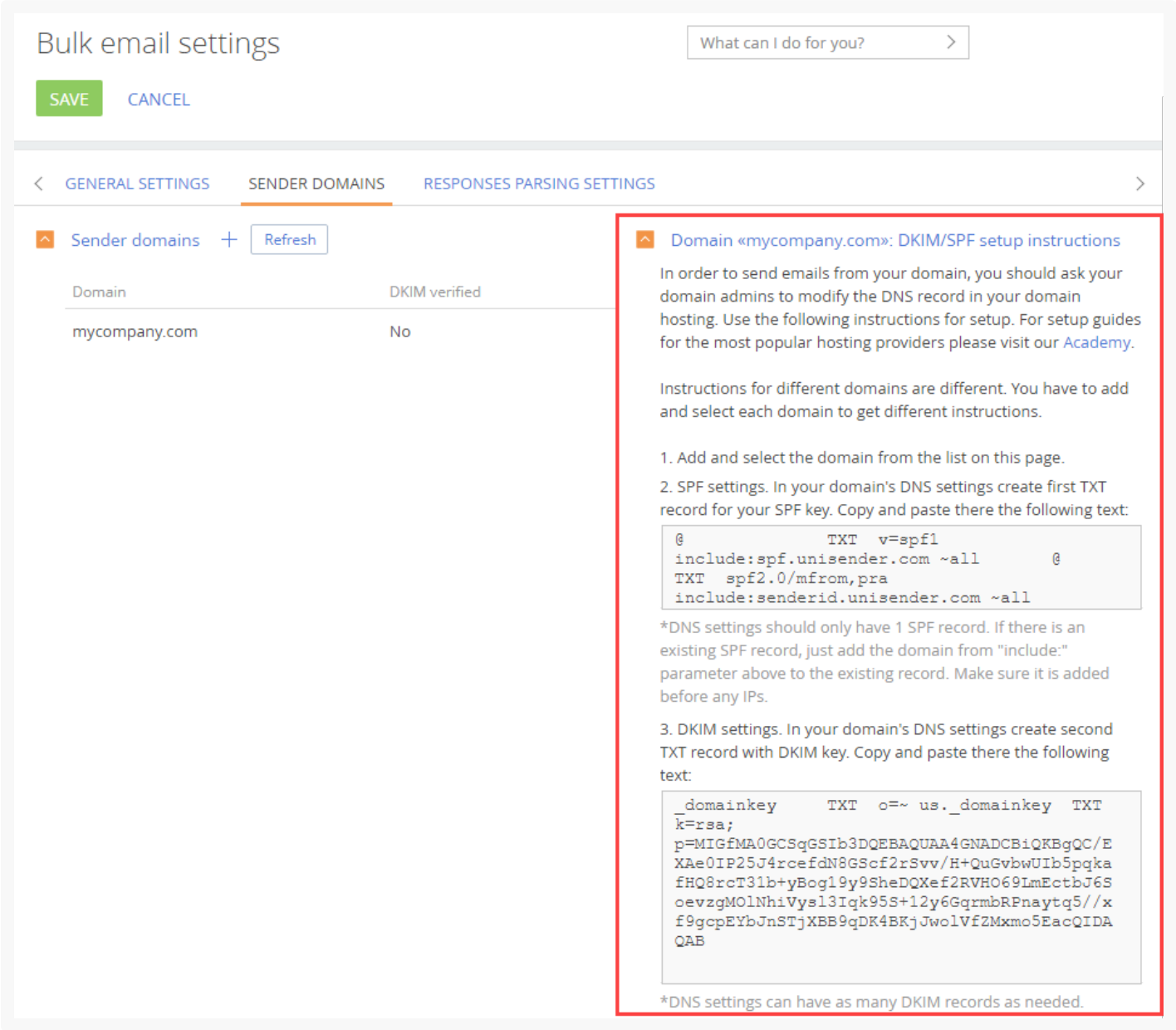

# Obtain SPF and DKIM records

SPF and DKIM records are generated automatically in the [ *Email* ] section once the domain is added to the email settings page.

To obtain these records, in the [ *Emails* ] section, select **Email settings** in the [ *Actions* ] menu.

The SPF and DKIM records will be generated automatically in the **DKIM/SPF setup instructions** area on the **Bulk email settings** page (Fig. 3) for your specified domain once your email is verified.

Fig. 3 SPF and DKIM keys for the specified domain




Elastic Email SPF and DKIM records are identical for all domains.

## Add the necessary records to the DNS area of your domain

To ensure high level of domain reputation and email deliverability, add the SPF, DKIM, Tracking Domain records and the DMARC policy to the DNS-zone of the email domain settings.

The setup procedure is as follows:

1. Specify SPF and DKIM records in the DNS area of your domain
2. If the DNS zone of your domain does not have an SPF record yet, you need to copy the generated SPF record from the [ *DKIM/SPF setup instructions* ] area on the **Email settings** page. The record will look as follows:

| Name | Type | Value |
|---|---|---|
| @ | TXT | v=spf1 a mx include:_spf.elasticemail.com ~all |

3. If you already have a TXT record with SPF information, then at the end of this record, before its last statement (for example, **?all**, **~all**, or **-all**), add the following line:

| Name | Type | Value |
|---|---|---|
| @ | TXT | include:_spf.elasticemail.com |

**Note.** Depending on the DNS editor, you may need to specify “@” and/or domain name the “Host / Name” field of the DNS zone. Contact your hosting provider for information about this value correct entering.

4. Specify the DKIM record in the DNS area of your domain For the Elastic Email provider this record will look as follows:

| Name | Type | Value |
|---|---|---|
| api._domainkey | TXT | k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbmGbQMzYeMvxwtNQoXN0waGYaciuKx8mtMh5czguT4EZlJXuCt6V+l56mmt3t68FEX5JJ0q4ijG71BGoFRkl87uJi7LrQt1ZZmZCvrEII0YO4mp8sDLXC8g1aUAoi8TJgxq2MJqCaMyj5kAm3Fdy2tzftPCV/lbdiJqmBnWKjtwIDAQAB |

**Note.** Certain DNS settings may require entering “api._domainkey.yourdomain.com” in the “Host / Name” field.

5. Specify SPF and DKIM records in the DNS area of your domain
To track the clicked link in the received email, Elastic Email overwrites the link address in the email template. When the recipient clicks to the link, the address with the domain "api.elasticemail.com" will be displayed in the browser first, and then the redirect to the link specified in the email will be performed. To specify your domain in the first link (for tracking), create the CNAME-record in the DNS settings of the domain:

| Name | Type | Value |
|---|---|---|
| tracking | CNAME | api.elasticemail.com |

6. Specify SPF and DKIM records in the DNS area of your domain
DMARC verification is only added after adding SPF and DKIM records and it provides the receiving server with the information upon further actions with emails from the unverified domain. Add a rule as TXT record of the DNS domain to activate DMARC:

| Name | Type | Value |
|---|---|---|
| _dmarc | TXT | v=DMARC1;p=none; |

The **v** tag specifies the protocol version, while **p** specifies the method of processing emails that have not been verified.

You can find more information about the protocol in the DMARC article of the Wikipedia. Detailed information about setting up the SPF and DKIM records, DMARC policy and the tracking domain is available in the instruction on the Elastic Email web site.

# Domain verification for the SendGrid provider

PRODUCTS: MARKETING

If you use SendGrid for sending marketing emails, you will need to verify your email address and your corporate domain to allow the provider to send emails on your behalf.

If your recipients use MS Outlook, Hotmail, Gmail, and other common mailing services, they can see that an email was sent from your provider's server on your behalf (this information is available in the “From” field).

**Note.** For example, if you are sending emails via SendGrid, the “From” field of the emails may contain the following text: “Your Manager <info@creatio.com> via sendgrid.net”.

The procedure for domain verification for SendGrid consists of several stages:

1. Add your corporate domain on the [ *Bulk email settings* ] page. Read more >>>
2. Obtain MX-, SPF-, and DKIM records. Read more >>>
3. Specify MX-, SPF-, and DKIM records in the DNS area of your domain Read more >>>

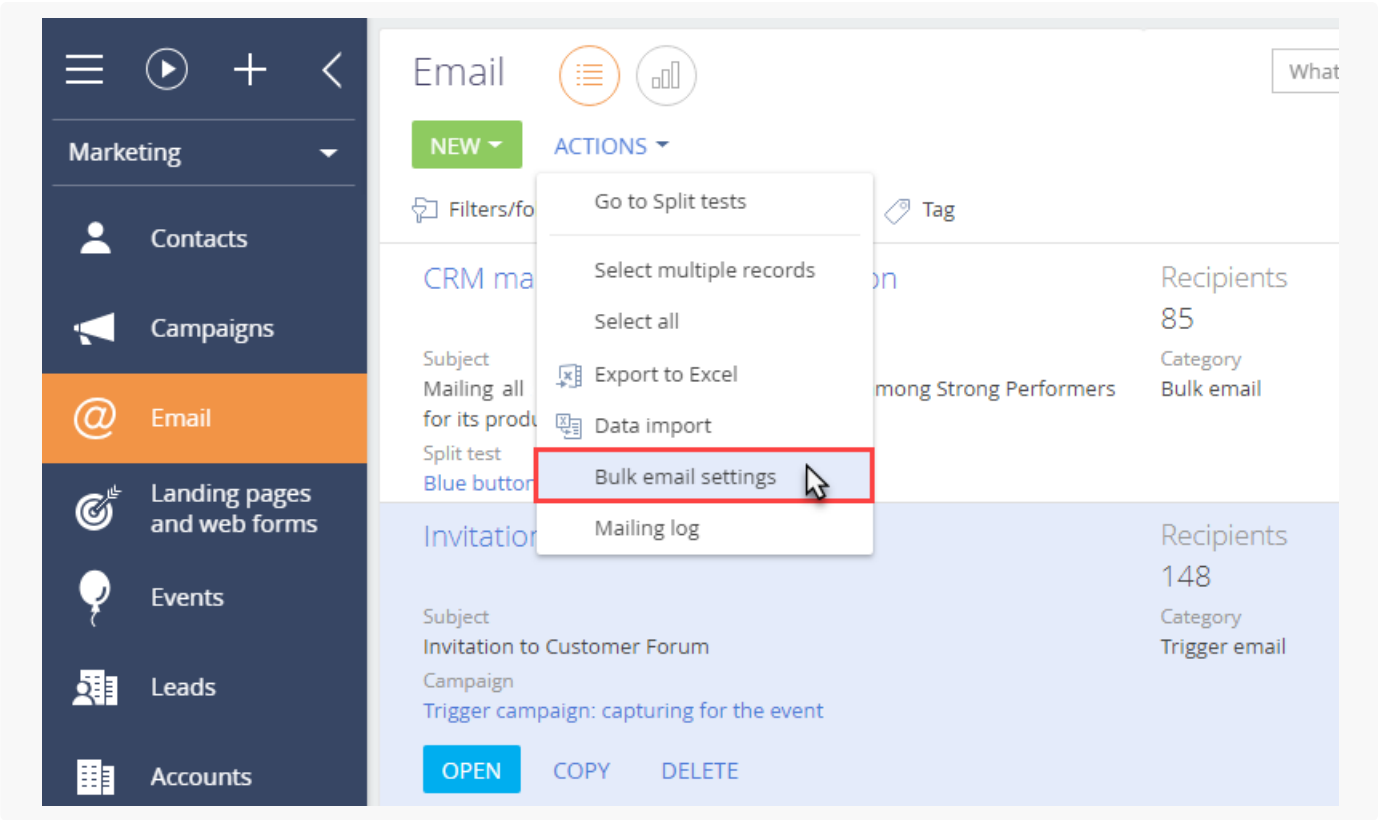
**Note.** Only custom email domains can be verified. Public domains (for example, gmail.com, yahoo.com, etc.) cannot be verified. We do not recommend using public domains for bulk emails. Such emails have a high risk of being marked as spam and ruining the reputation of the sender IP address.

## Add your corporate domain on the [ *Bulk email settings* ] page

SendGrid users need to add their corporate domain to Creatio before starting their emails. To do so:

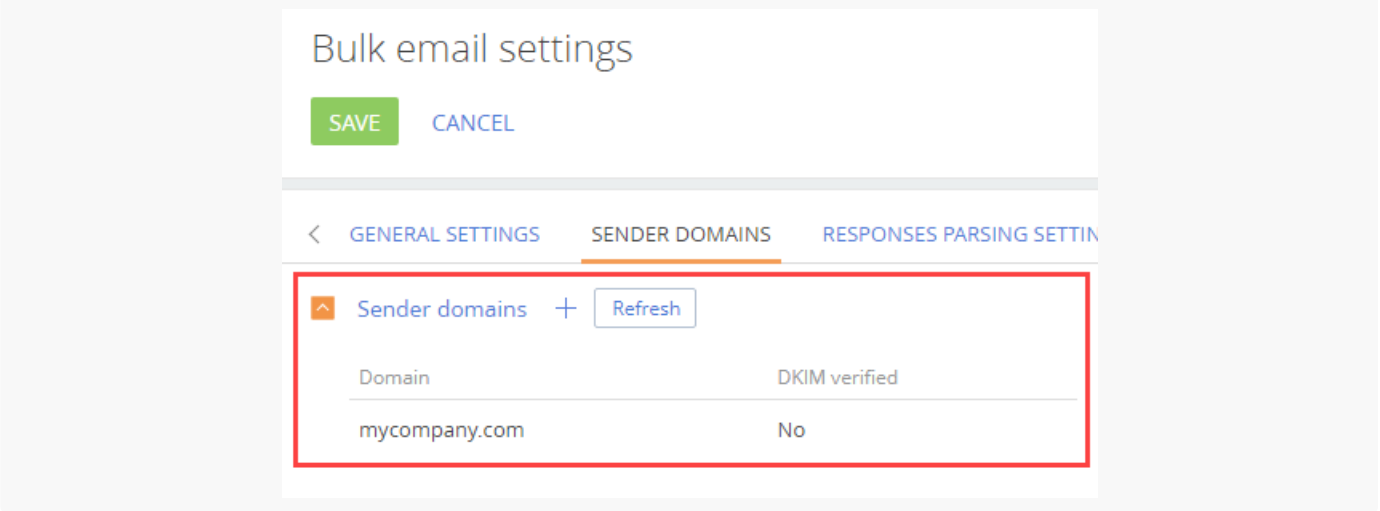
1. In the **Emails** section, select **Bulk email settings** in the **Actions** menu (Fig. 1)

Fig. 1 Opening the bulk email settings page




2. On the **Bulk email settings** page, specify the domain of the necessary email address in the **Sender domain** area, i.e., “mycompany.com” (Fig. 2).

Fig. 2 The [ *Sender domains* ] tab

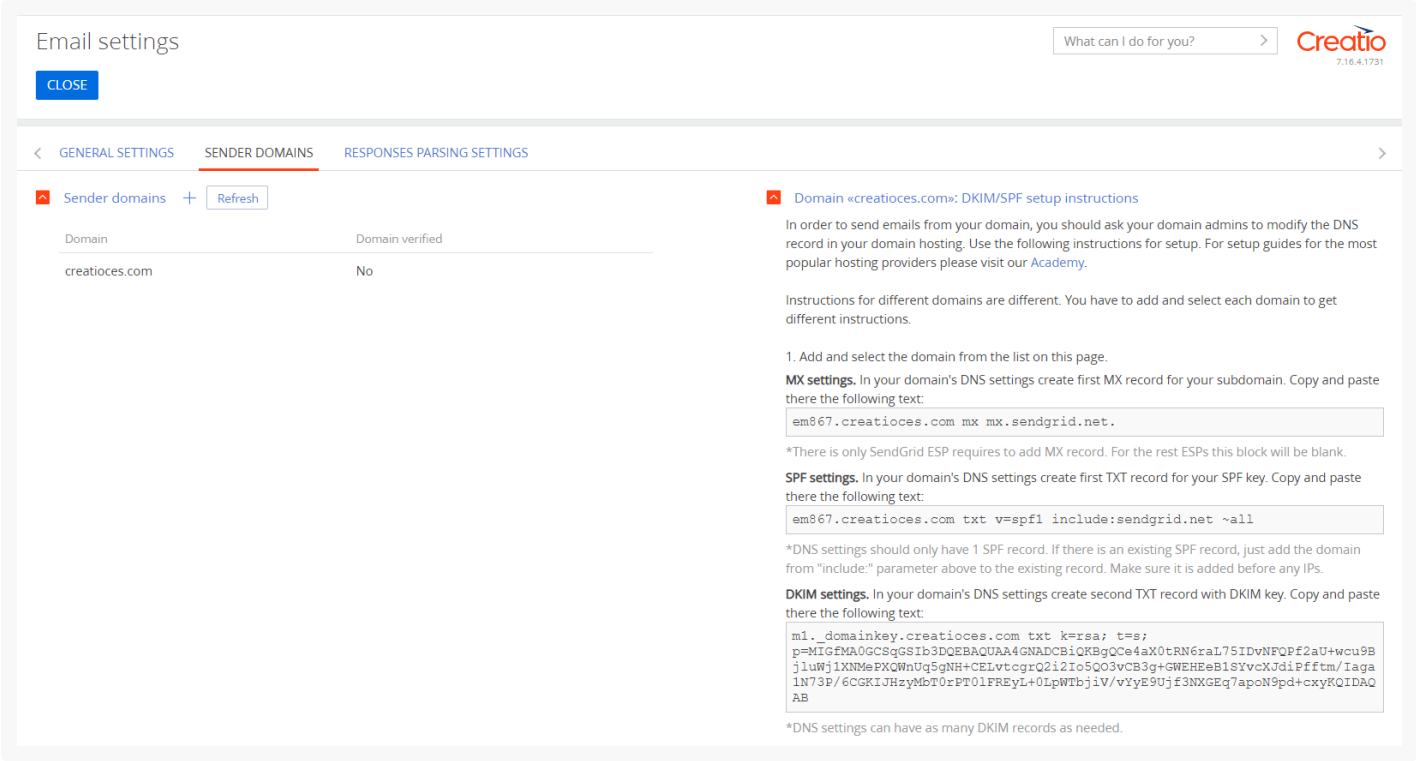



## Get setup keys for your domain

MX-, SPF- and DKIM records are generated automatically in the **Email** section once the domain is added to the email settings page. To obtain these records, in the **Email** section, select **Email settings** in the [ *Actions* ] menu.

The SPF and DKIM records will be generated automatically in the **DKIM/SPF setup instructions** area on the **Bulk email settings** page (Fig. 3) for your specified domain once your email is verified.

Fig. 3 MX/DKIM/SPF keys for the specified domain




**Attention.** MX-, SPF- and DKIM records of the SendGrid provider are different for different domains.

# Add records to the DNS area of your domain

To verify the mail domain using the SendGrid provider, you need to add the MX, SPF to the DNS area of the mail domain settings, otherwise, the domain reputation and the mail delivery quality are not guaranteed.

**Note.** We recommend looking into the examples provided in the Recommendations on setting up the popular DNS providers article.

Specify MX record in the DNS area of your domain

**MX record** is the primary record in the domain zone; it specifies mailing host names of the domain. The email server checks if MX records are available in the DNS zone and whether they match the sender's IP address. If the data is unavailable or the IP addresses do not match, the remote server is very likely to deny sending and receiving emails.

Unlike SPF and DKIM records, the syntax of MS records includes priorities. **Priority** is specified as an integer; it indicates the order in which the availability of email servers is checked. The highest possible priority is "0." You can add several MS records with equal priority.

An MX record looks like this:

| Name | Priority | Type | Value |
|---|---|---|---|
| subdomain.yourdomain.com | 0 | mx | mx.sendgrid.net. |

The subdomain name is unique and is generated by the provider.

### Specify SPF record in the DNS area of your domain

Copy the generated SPF record from the **DKIM/SPF setup instructions** area on the **Bulk email settings** page, which will look as follows: The record will look as follows:

| Name | Type | Value |
|---|---|---|
| subdomain.yourdomain.com | TXT | v=spf1 a mx include:_spf.sendgrid.com ~all |

The subdomain name is unique and is generated by the provider. Add a separate record for each subdomain.

### Specify DKIM record in the DNS area of your domain

After the configuration of the SPF record, you need to add DKIM records. For the SendGrid provider, the record should look like this:

| Name | Type | Value |
|---|---|---|
| m1._domainkey | TXT | k=rsa; t=s; p=XXXXXXXXXXXXX |

In the record above, “XXXXXXXXXXXXX” is an **individual key** for each domain. The key is generated automatically and is available on the **Sender domains** tab.

Certain DNS settings may require entering the provided subdomain in the “Host / Name” field in the following format: “m1._domainkey.yourdomain.com”

**Note.** Detailed information about MX, SPF, and DKIM record setup is available in the SendGrid online guide.

# Recommendations on setting up the popular DNS providers

PRODUCTS: MARKETING

Please consider the following when working with SPF and DKIM records:

1. Before the changes made to the DNS records of your email domain take effect, the domain provider must verify new and modified records. The verification time differs depending on the provider and usually takes

several hours due to caching. You can learn more in your domain server documentation.

2. Some records may not pass the verification. This may occur due to differences in DKIM record formatting requirements of various domain providers. For example, certain providers require the “\” character before “;” at the start and end of DKIM records, while others have no such requirements.
3. Before you add a DKIM record, obtain formatting requirements from the documentation or support service of your domain provider to ensure the record complies with them.

View links to the websites of common domain providers and their DKIM record formatting specifics in the table below.

| | |
|---|---|
| Bluehost | DKIM records are usually formatted automatically (control characters are automatically replaced with corresponding text characters). |
| GoDaddy | DKIM records are usually formatted automatically (control characters are automatically replaced with corresponding text characters). |
| CloudFlare | DKIM records are usually formatted automatically (control characters are automatically replaced with corresponding text characters). |
| GSuite/GoogleWorkspace, | DKIM records are usually formatted automatically (control characters are automatically replaced with corresponding text characters). |
| DynDNS | The field where you enter the value of each record must be enclosed in double quotes. |
| MS Office 365 | DKIM records are usually formatted automatically (control characters are automatically replaced with corresponding text characters). |

**Note.** Only custom email domains can be verified. Public domains (for example, gmail.com, yahoo.com, etc.) cannot be verified. We do not recommend using public domains for bulk emails. Such emails have a high risk of being marked as spam and ruining the reputation of the sender IP address.

# Set up the SPF and DKIM records in MS Office 365

## SPF setup

To use a custom domain in Microsoft 365, add an SPF text record to DNS settings, using commands from the table:

| **Any mail system (required)** | **v=spf1** |
|---|---|
| Exchange Online | include:spf.protection.outlook.com |
| Only for Exchange Online | ip4:23.103.224.0/19 ip4:206.191.224.0/19 ip4:40.103.0.0/16 include:spf.protection.outlook.com |
| Microsoft 365 Germany, only Microsoft Cloud Germany | include:spf.protection.outlook.de |
| Third-party mail system | Include:<domain name>, where <domain name> is the domain of the third-party mail system. |
| Local mail system, such as Exchange Online Protection with a different mail system | Use one of the following parameters for each additional mail system:<br>ip4:<IP address><br>ip6:<IP address><br>include:<domain name><br>where <IP address> is the mail system IP address and <domain name> is the mail system domain. |
| Any mail system (required) | This can be one of several values. Using the -all value is recommended. |

For example, if your organization uses only Microsoft 365 and you do not have local mail servers, your SPF record should look like this:

```
v=spf1 include:spf.protection.outlook.com -all
```

This is one of the more common SPF record formats for Microsoft 365. This record will be accepted in most cases, regardless of the location of your Microsoft 365 (the USA or Europe, including Germany, or anywhere else).

After creating an SPF record, update it in the DNS service. Only one SPF record can exist for a domain. If the record already exists, update it instead of adding a new record.

After adding an SPF record, verify it. More information about the SPF verification process is available on the Microsoft website.

## DKIM setup

On the provider’s side, add CNAME records for additional domains and enable DKIM in Microsoft 365.

1. Adding CNAME records

   Each additional domain requires two CNAME records. A CNAME record specifies that the domain name is an alias of another domain. Use the following format:

| | |
|---|---|
| Host name | selector1._domainkey.<domain>. |
| Points to address or value | selector1-<domainGUID>._domainkey.<initialDomain>. |
| TTL | 3600 |
| Host name | selector2._domainkey.<domain> |
| Points to address or value | selector2-<domainGUID>._domainkey.<initialDomain> |
| TTL | 3600 |

In this example, selector1 and selector2 are selectors for Office 365. The selector names do not change.

The domainGUID value matches the domainGUID value specified for mail.protection.outlook.com in custom MX record for the personal domain. For example, in the creatio1-com.mail.protection.outlook.com record, it is creatio1-com.

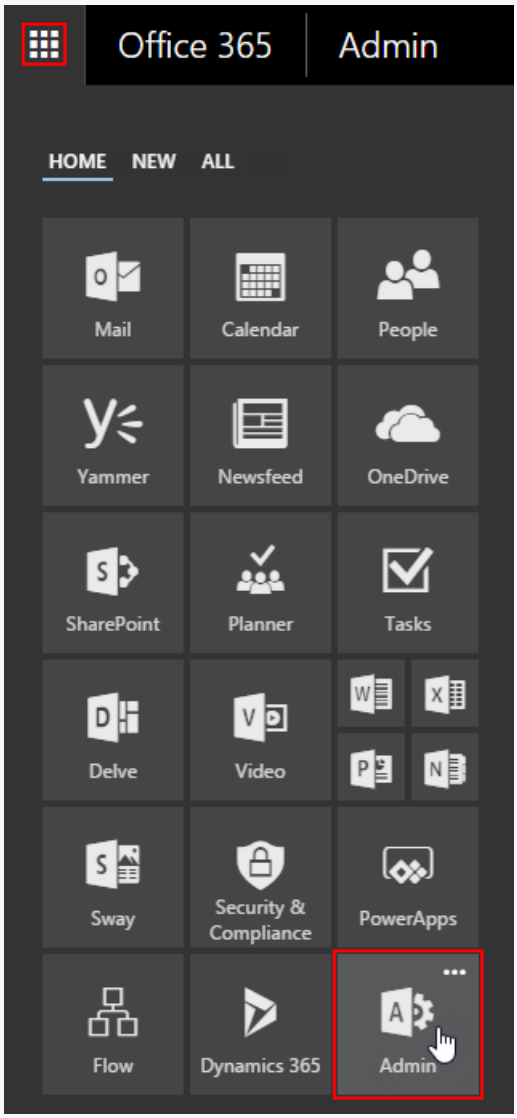
The initialDomain value matches the domain that you used when registering in Office 365.

2. Enabling DKIM

   After adding CNAME records to DNS, enable DKIM signature in Office 365.

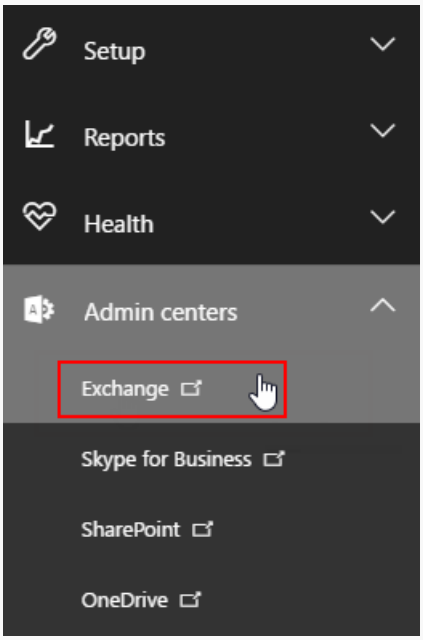
   In the upper-left corner of the Office 365, click the application icon and select “Administrator” (Fig. 1).

Fig. 1 Opening administrator menu



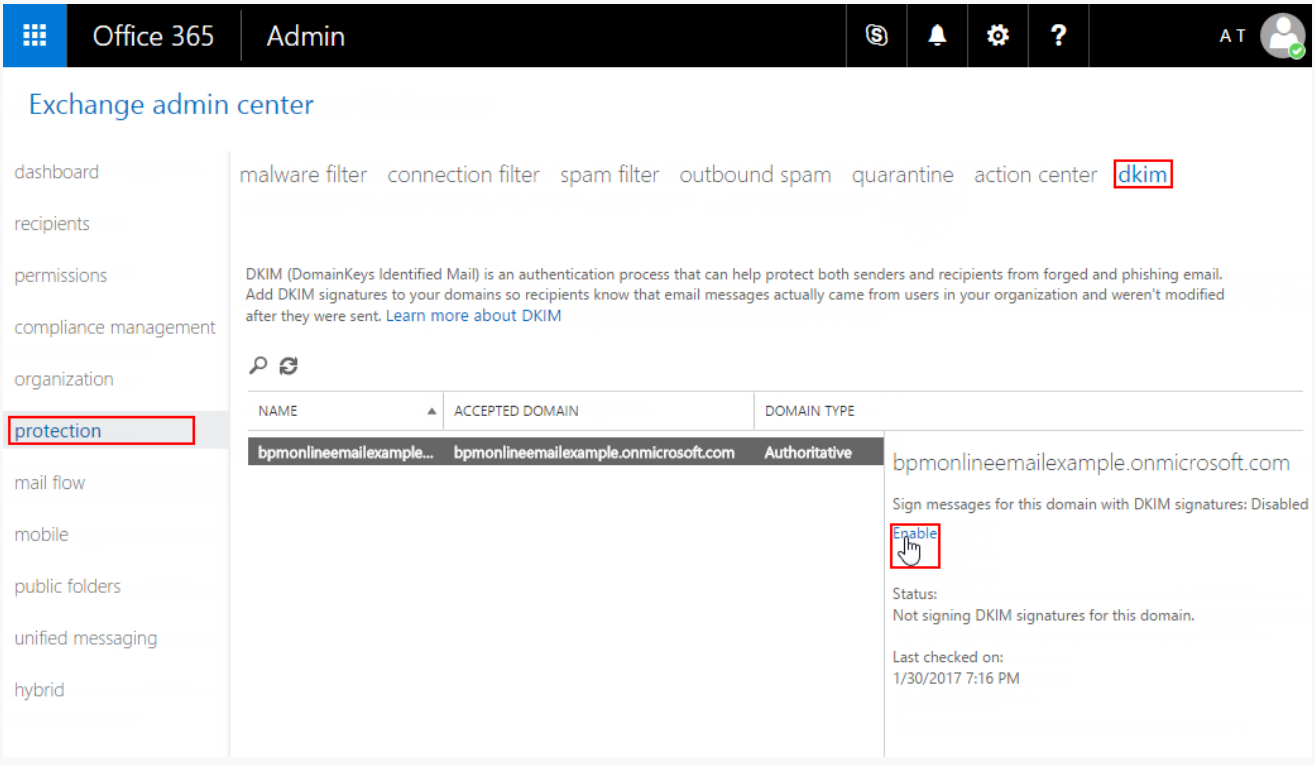

3. In the navigation area, select “Admin centers” > “Exchange” (Fig. 2).

Fig. 2 Opening Exchange




4. Open the “Protection” section and select the “dkim” tab. Select the domain, for which to enable DKIM in the list of domains, then click “Enable” (Fig. 3) under “Sign messages for this domain with DKIM signatures”.

Fig. 3 Enabling DKIM for domain




5. Repeat this step for each domain.