Creatio Academy

Recommendations for DNS

Recommendations on setting up the popular DNS providers

Version 8.0

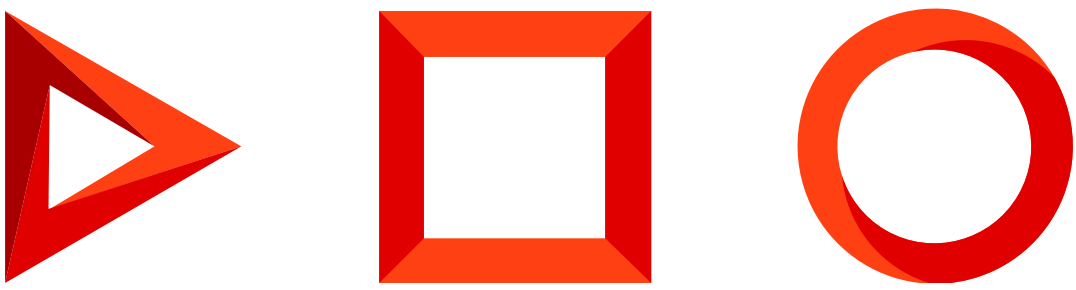


Table of Contents

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: ip4:<IP address> ip6:<IP address> include:<domain name> 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.

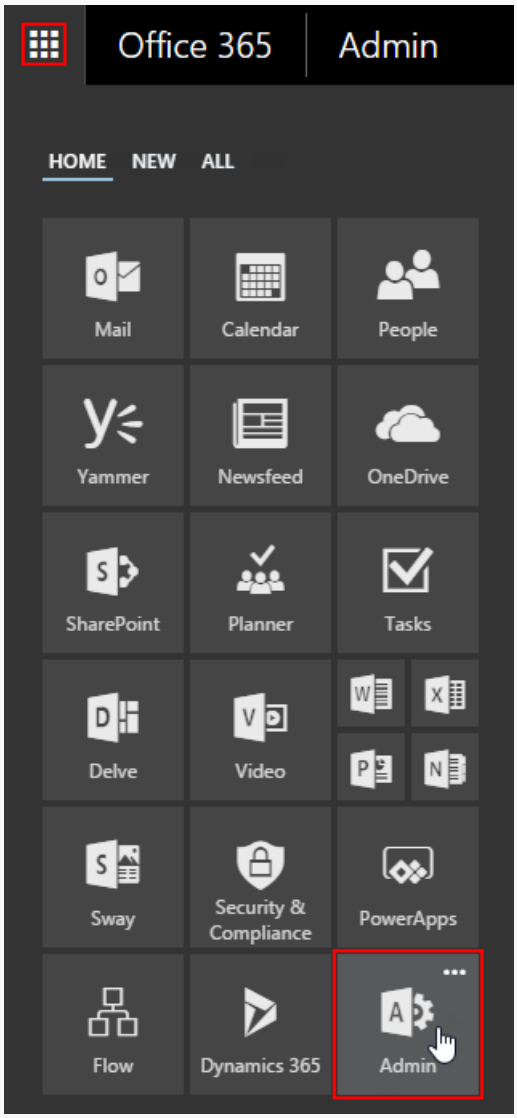
   The initialDomain value matches the domain that you used when registering in Office 365.

2. Enabling DKIM

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

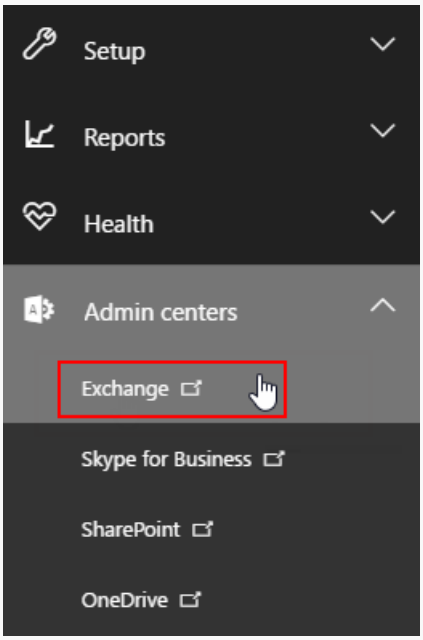
   In the upper-left corner of the Office 365, click the application icon and select "Administrator" (Fig. 1).

Fig. 1 Opening administrator menu



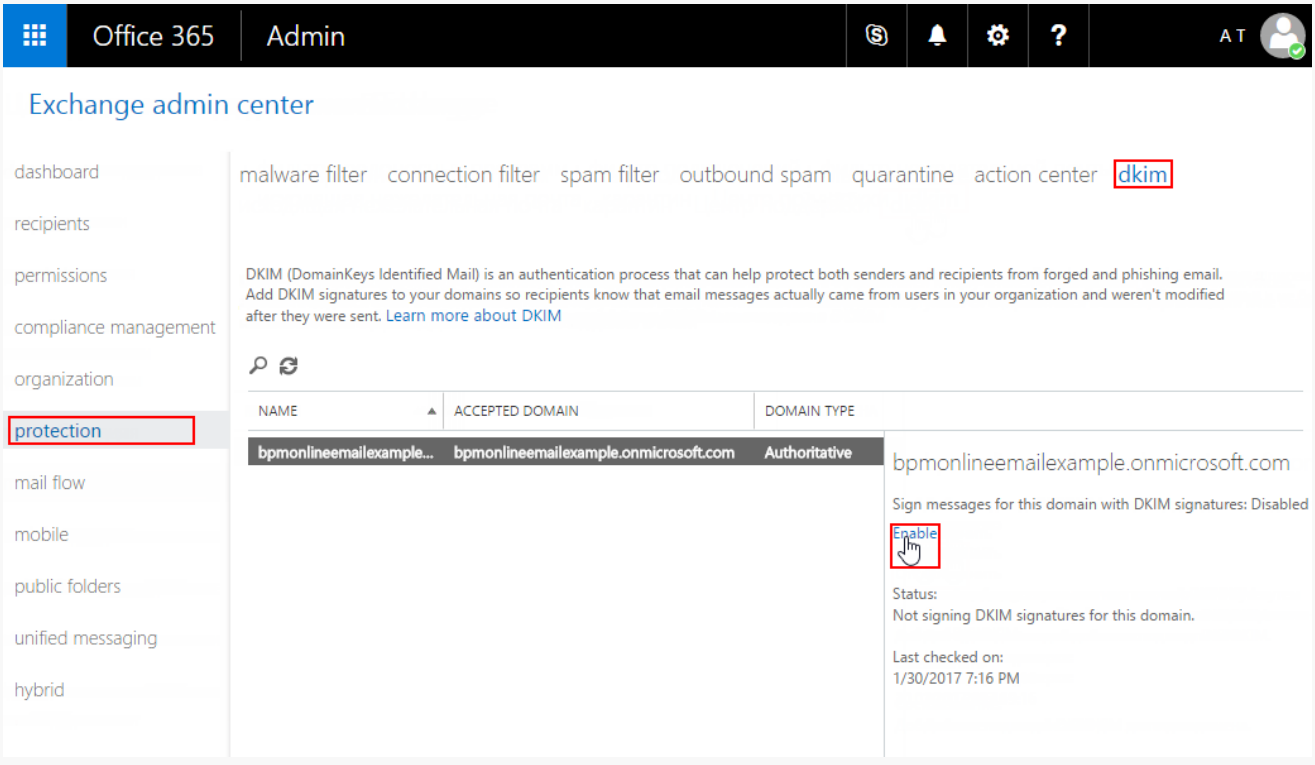
3. In the navigation area, select “Admin centers” > “Exchange” (Fig. 2).

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.