|  |
| --- |
| Securing your email domain |

Contents

[Background 2](#_Toc169188459)

[SPF (Sender Policy Framework) 2](#_Toc169188460)

[DMARC (Domain-based Message Authentication, Reporting & Conformance) 2](#_Toc169188461)

[DKIM (DomainKeys Identified Mail) 2](#_Toc169188462)

[What you will need to do as an organization using Microsoft 365 2](#_Toc169188463)

[Check your current configuration 3](#_Toc169188464)

[Update your email protection 3](#_Toc169188465)

[Set up SPF and DKIM records 3](#_Toc169188466)

[Enable DKIM 3](#_Toc169188467)

[Set up DMARC 3](#_Toc169188468)

[Verify your changes 4](#_Toc169188469)

[What you will need to do as an organization using Google Workspace 4](#_Toc169188470)

[Check your current configuration 4](#_Toc169188471)

[Update your email protection 4](#_Toc169188472)

## Background

Large email providers like Google and Microsoft may block your emails if you don’t meet a minimum level of trust. You will need to configure your domain with specific DNS records that ensure your email domain is securely authenticated and can be trusted.

SPF, DMARC and DKIM are email authentication protocols that prevent email spoofing and improve email delivery rates.

## SPF (Sender Policy Framework)

What it is: Think of SPF as a list of who is allowed to send emails on behalf of your domain (eg, example.com).

Why it's important: It helps prevent email spoofing, where someone sends an email pretending to be you.

## DMARC (Domain-based Message Authentication, Reporting & Conformance)

**What it is:** DKIM is a way to make sure that an email actually comes from the domain it says it’s from and hasn’t been tampered with during its journey.

**Why it’s important:** DKIM helps to prove that an email was genuinely sent from the domain it claims to be from. This helps prevent email spoofing, where someone sends an email pretending to be from someone else’s domain. It also ensures that the email content hasn’t been altered while in transit (email integrity).

## DKIM (DomainKeys Identified Mail)

**What it is:** DKIM is a way to make sure that an email actually comes from the domain it says it’s from and hasn’t been tampered with during its journey.

**Why it’s important:** DKIM helps to prove that an email was genuinely sent from the domain it claims to be from. This helps prevent email spoofing, where someone sends an email pretending to be from someone else’s domain. It also ensures that the email content hasn’t been altered while in transit (email integrity).

## What you will need to do as an organization using Microsoft 365

**Please note:** The steps below should only be performed by an experienced IT professional who understands DNS. There is significant risk involved in executing these steps, so be cautious and ensure you have a backup.

## Check your current configuration

Use the following online email configuration checker to make sure you have the basics in place for SPF and DMARC: [DMARC Domain Checker](https://dmarcian.com/domain-checker/)

## Update your email protection

### Set up SPF and DKIM records

Microsoft provides a wizard for helping you to set up your email-related DNS records including SPF and DKIM. You will need to add DMARC manually.

1. Login to the [Microsoft 365 admin centre](https://admin.microsoft.com).
2. Go to **Settings** > **Domains** (if you don’t see the settings option, click on **Show all** in the left-hand navigation).
3. Click on the domain you want to update. Depending on how this was left after the original setup of Microsoft 365 you may see different options. If the domain setup process wasn’t completed you will get a **Continue setup** option. Otherwise, you will see several tabs, one of which is **DNS records**.
4. Click on **DNS records** (or **Continue setup**).
5. If using the **Continue setup** option, the wizard will automatically start. Otherwise click on **Manage DNS** to launch it.
6. When you get to the **Add DNS records** screen, expand the **Advanced options** menu at the bottom and make sure **DomainKeys Identified Mail (DKIM)** is selected.
7. Follow the wizard instructions.

### Enable DKIM

Once the DKIM DNS records are added you need to enable the signing of emails.

1. Go to the [Microsoft Security Centre](https://security.microsoft.com).
2. Go to **Email & Collaboration** > **Policies & rules** > **Threat Policies** > **Email Authentication Settings** > **DKIM**.
3. Click on the domain you want to enable DKIM for. If this is the first time you’ve looked at DKIM for your domain, you will see an option to enable DKIM. Turn this on. Once this is enabled you will have an option to **Sign messages for this domain with DKIM signatures**. Turn this on. Your DNS records will be confirmed and if everything checks out DKIM is enabled.

### Set up DMARC

1. Login to your DNS provider:
* Go to your DNS host provider's website (such as GoDaddy, Namecheap, etc) and sign in to your account.
1. Access DNS settings:
* Select the domain you want to update.
* Find the DNS settings or DNS management section.
* Add DMARC record: Add a new **TXT** record with the following details:

|  |
| --- |
| **Type:** TXT**Name:** \_dmarc**TTL:** 3600 (or leave it at the default value)**Value/Data:** v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s  |

**Note:** There are numerous options for the DMARC record. If you only use Microsoft 365 for your email, then the above provides a good secure baseline. You will need to customise the record if you have a more complex environment – this is beyond the scope of this guide.

1. Add a reporting mailbox to your DMARC Policy (optional):
* It is a good idea to set up a shared mailbox to receive DMARC reports. This allows you to see misuse of your domain. Change the value of your DMARC record to:

|  |
| --- |
| **Quarantine:** v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:*dmarc-reports@yourdomain.com* |

* Replace dmarc-reports@yourdomain.comwith the email address for your shared mailbox.
1. Save the record.

### Verify your changes

1. Propagation time:
* DNS changes may take some time to propagate, typically from a few minutes up to 48 hours.
1. Check your records:
* Use online tools like [MXToolbox](https://mxtoolbox.com/) or a [DMARC Analyzer](https://dmarcian.com/domain-checker/) to verify that your SPF and DMARC records are correctly configured.

## What you will need to do as an organization using Google Workspace

**Please note:** The steps below should only be performed by an experienced IT professional who understands DNS. There is significant risk involved in executing these steps, so be cautious and ensure you have a backup.

## Check your current configuration

Use the following online email configuration checker to make sure you have the basics in place for SPF and DMARC: [DMARC Domain Checker](https://dmarcian.com/domain-checker/)

## Update your email protection

#### Set up SPF record

Login to your DNS provider:

Go to your DNS host provider's website (such as GoDaddy, Namecheap, etc) and sign in to your account. If you registered your domain with Google, you can manage your DNS records through [Google Domains](https://domains.google.com/).

Access DNS settings:

Select the domain you want to update.

Find the DNS settings or DNS management section.

Add or update SPF record:

Look for an existing SPF record (a TXT record starting with "v=spf1"). If there is one, you will need to update it. If there isn’t, you will need to add a new TXT record.

Add a new **TXT** record or edit the existing one with the following details:

|  |
| --- |
| **Name:** @ (or leave it blank, depending on your DNS host)**Type:** TXT**TTL:** 3600 (or leave it at the default value)**Value/Data:** v=spf1 include:\_spf.google.com ~all |

If you have multiple sources that send email for your domain, you can include them as well. For example:

|  |
| --- |
| * v=spf1 include:\_spf.google.com include:anotherdomain.com ~all
 |

Save the record.

#### Set up DMARC record

Add DMARC record:

In the same DNS settings area, add a new **TXT** record with the following details:

|  |
| --- |
| **Name:** \_dmarc**Type:** TXT**TTL:** 3600 (or leave it at the default value)**Value/Data:** v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com |

Modify DMARC Policy (optional):

For stricter enforcement, you can change the p value:

|  |
| --- |
| **Quarantine:** v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com**Reject:** v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com |

You can also specify where to send aggregate and forensic reports by adding ruf for forensic reports:

|  |
| --- |
| v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-forensic@yourdomain.com |

Save the record.

#### Set up DKIM

To set up DKIM (DomainKeys Identified Mail) for your domain in Google Workspace, you'll need to generate DKIM keys in the Google Admin console and then update your DNS records with your domain host. Here’s how you can do it:

**Step 1: Generate DKIM keys in Google Admin Console**

Login to Google Admin Console:

Go to the [Google Admin Console](https://admin.google.com/) and sign in with your admin credentials.

Navigate to DKIM settings:

In the Admin console, go to Apps > Google Workspace > Gmail > Authenticate email.

Select your domain:

If you have multiple domains, select the domain for which you want to set up DKIM.

Generate a DKIM key:

Click on Generate new record.

Select the DKIM key bit length. Google recommends using a 2048-bit key for better security.

Click Generate.

Copy the DNS Hostname and TXT record:

After generating the key, you will see the **DNS Hostname** and **TXT record value**. Copy these values as you will need them for the next step.

**Step 2: Add DKIM DNS record at your domain host**

Login to your DNS provider:

Go to your DNS host provider's website (such as GoDaddy, Namecheap, etc) and sign in to your account. If you registered your domain with Google, you can manage your DNS records through [Google Domains](https://domains.google.com/).

Access DNS settings:

Select the domain you want to update.

Find the DNS settings or DNS management section.

Add DKIM TXT record:

Add a new **TXT** record with the following details:

|  |
| --- |
| **Name/Host/Alias:** This will be the **DNS Hostname** you copied from the Google Admin console. It usually looks like google.\_domainkey.**Type:** TXT**TTL:** 3600 (or leave it at the default value)**Value/Data:** This will be the **TXT record value** you copied from the Google Admin console. It looks like a long string starting with v=DKIM1; k=rsa; p=.... |

Save the record.

**Step 3: Enable DKIM signing**

Return to Google Admin Console:

Go Google Admin Console > Apps > Google Workspace > Gmail > Authenticate email.

Enable DKIM:

In the DKIM settings, after adding the DNS record, click on **Start authentication**.

Google will verify the DNS record. Once verified, DKIM will be enabled for your domain.

#### Verify your changes

Propagation time:

DNS changes may take some time to propagate, typically from a few minutes up to 48 hours.

Check your records:

Use online tools like [MXToolbox](https://mxtoolbox.com/) or [DMARC Analyzer](https://www.dmarcanalyzer.com/) to verify that your SPF, DMARC and DKIM records are correctly configured.