

# DMARC Guide

Microsoft 365 and  
Google Workspace



September 2024

# Acknowledgments

CIS would like to recognize the following individuals and organizations for their support. Their time and expertise were a vital component of completing this important work.

## Editor

Phil White, CIS

## Contributors

Caleb Eifert, CIS

Edward Byrd, CIS

Joshua Stankus, CISA

# Contents

## Introduction 1

---

Why is DMARC Important? 2

How SPF, DKIM, and DMARC Work Together 3

How to Rollout DMARC 6

## Google Workspace Configuration 9

---

DKIM Configuration 9

Configure SPF in DNS Record 10

Configure DMARC in DNS Record 11

Additional Information 12

## Microsoft 365 Configuration 13

---

Configure DKIM in Microsoft 365 13

Configure SPF in DNS Record 14

Additional Information 17

## Conclusion 18

---

## Appendix 19

---

Third-party Email Providers 19

Additional Information 19

# Introduction

Email is one of the most widely used and effective communication channels in the modern world. But it also faces many challenges and threats from cybercriminals who exploit this channel to launch phishing, spoofing, and spamming attacks. To combat this, many email services are implementing Domain-based Message Authentication, Reporting, and Conformance (DMARC) on sent emails. DMARC is a key component of email security strategy. It helps prevent phishing scams, spam, and other email security risks by allowing recipients to trust that messages came from the authenticated domain owner, not an impostor.

To benefit from this, senders also need to support DMARC, but setting it up correctly is not a trivial task. It requires careful configuration and monitoring of Domain Name System (DNS) records, alignment of Send Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) identifiers, testing of various DMARC policies, and analysis of DMARC reports.

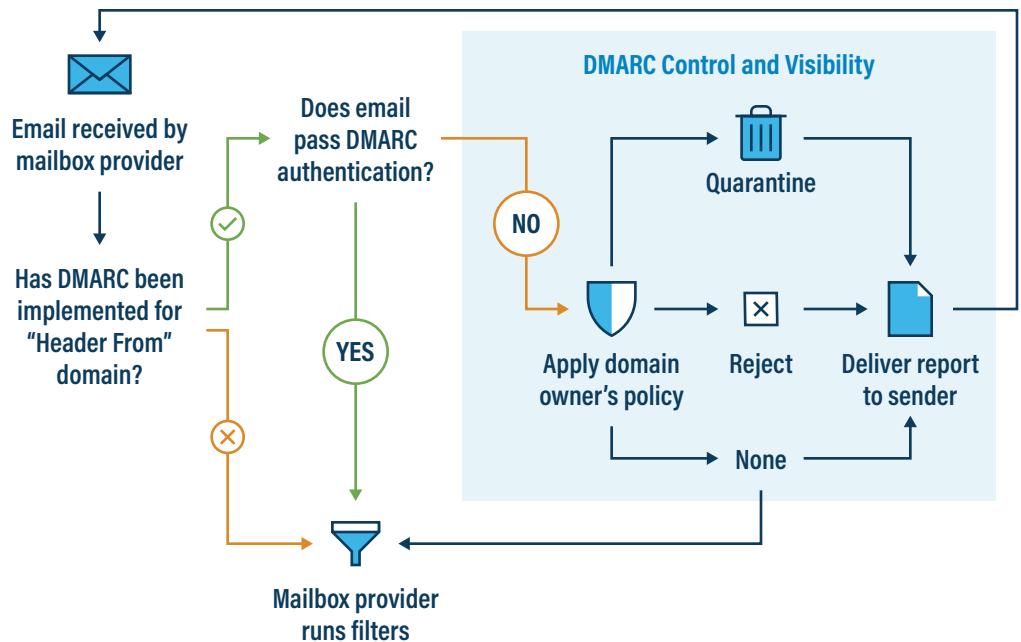
Failing to properly setup DMARC on the sender side can result in legitimate emails being blocked or marked as spam, which can hurt email deliverability and performance. That’s why it is essential for organizations that rely on email communication to understand the benefits and challenges of DMARC and how to implement it properly.

	Description	Benefit
SPF	A DNS record that specifies which IP addresses are authorized to send email from a domain.	Prevents unauthorized use of a domain by spammers or spoofers.
DKIM	A digital signature embedded in the email header that proves the message was sent by the domain owner and was not tampered with in transit.	Ensures the authenticity and integrity of the email message.
DMARC	A DNS record that defines how SPF and DKIM results should be interpreted by a receiving email server and what suggested action the receiver should take if the email fails authentication checks.	Enables domain owners to monitor and control how their domains are used in email communication.

DMARC is the first and only widely deployed technology that can make the “From:” header domain (what users see in their email clients) trustworthy. By using DMARC, domain owners can prevent their domains from being used in phishing or spoofing attacks that target their customers, employees and partners.

This document will cover how to set DMARC up for Microsoft 365 and Google Workspace email to work smoothly with the MS-ISAC/EI-ISAC Email Protection Service (EPS).

**Figure 1. How DMARC Works**



## Why is DMARC Important?

Phishing emails are always changing, making it difficult for people to recognize them. Spam filters will block incoming email by using various algorithms to constantly monitor and detect email spam trends.

The biggest difference between DMARC and spam filters is that DMARC keeps receivers of email safe from fake emails that use a sender's domain name. With a spam filter, only that protected inbox is safe from phishing emails. DMARC uses email authentication protocols to ensure that if an attacker tries to impersonate your organization and send emails, any receiving server can detect this and potentially block them.

This means that not just the receiver is protected from phishing attacks, but the sending organization's image and reputation is also being safeguarded. When DMARC is enforced, attackers won't be able to impersonate the organization's domain to send emails internally (to the organization's employees) or externally (to the public).

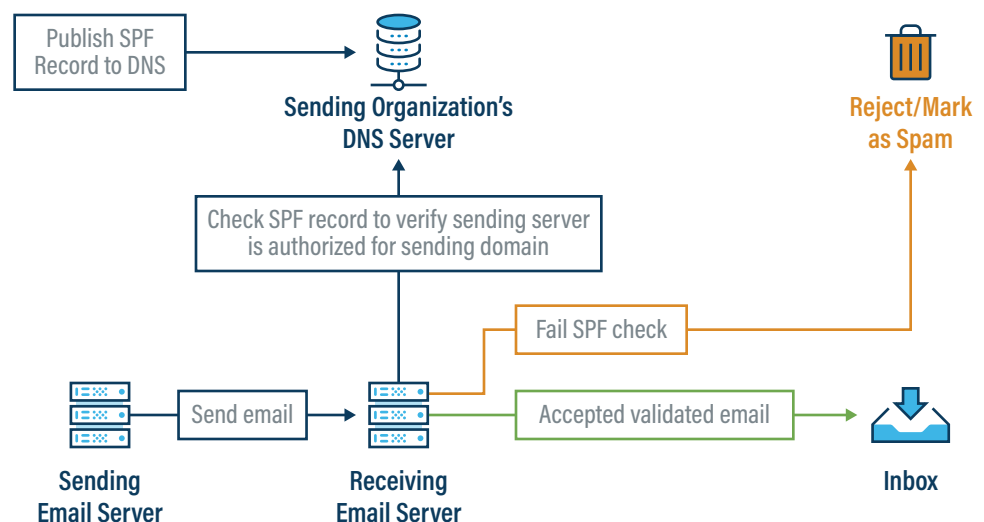
## How SPF, DKIM, and DMARC Work Together

These mechanisms were created at different times and address different parts of the overall bad email problem.

### SPF

SPF tells receiving email servers what email sending servers are allowed to send email on behalf of an organization (allowed domain(s)) via a DNS record entry registered for the sending organization's domain.

**Figure 2. How SPF Works**

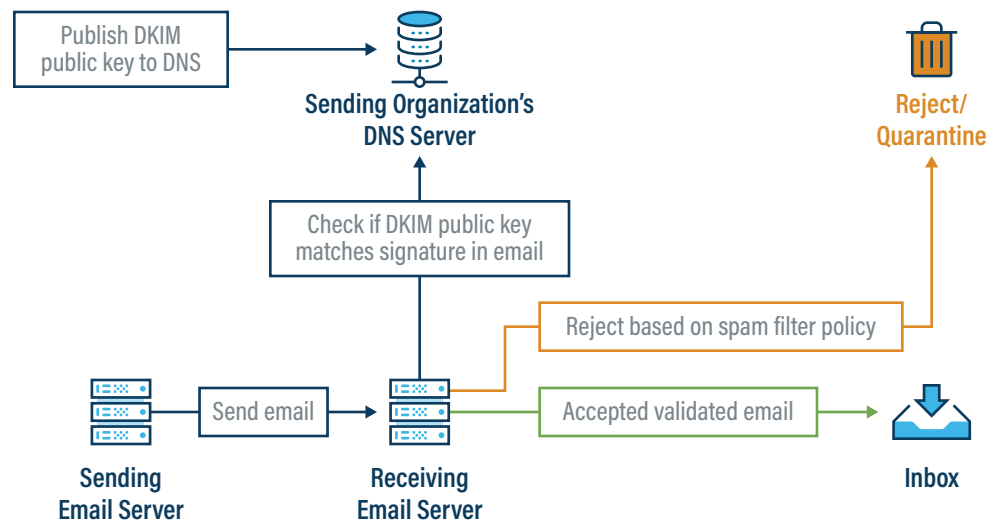


The receiving email server can decide what to do with the incoming email based on its configured policy (Reject, Quarantine, mark as spam, etc.). These settings are typically receiving email server specific.

## DKIM

DKIM is a process that signs all outgoing email messages with a private key; receiving email servers can access the corresponding public key for the sending organization from their DNS record.

**Figure 3. How DKIM Works**

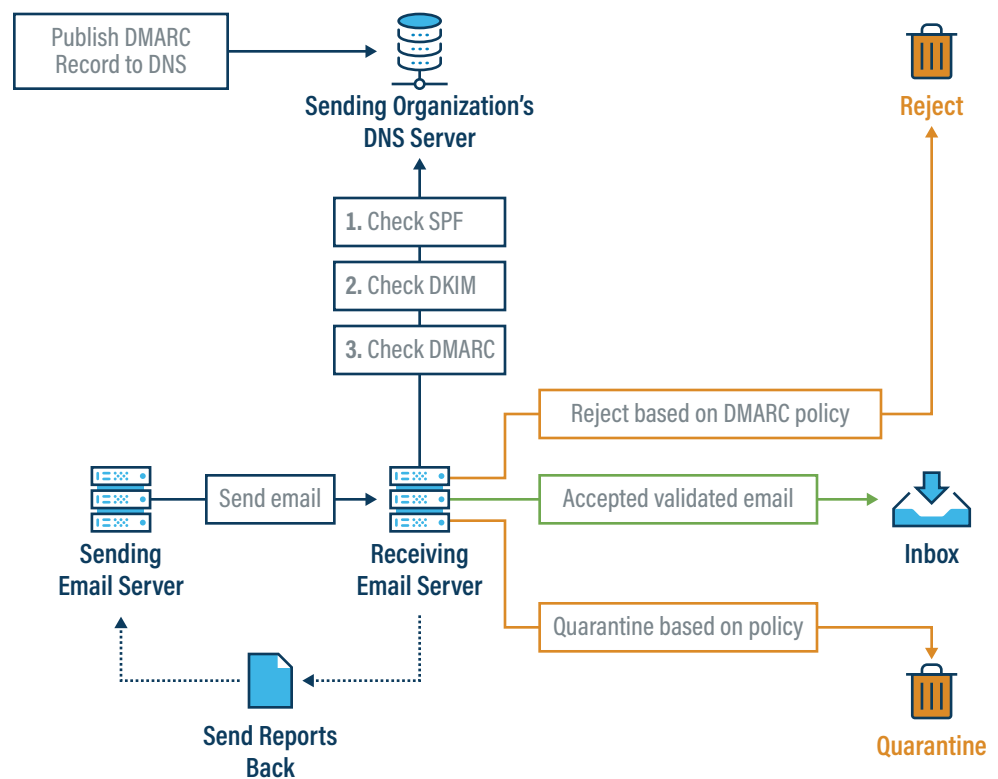


The receiving email server can decide what to do with the incoming email based on its configured policy (typically Reject or Quarantine) These settings are typically receiving email server specific.

## DMARC

DMARC ties SPF and DKIM together and allows domain owners sending email to tell receiving email servers how to process email that claim to come from sender's domain that did not align with SPF or DKIM. Also, it allows domain owners that send email to get reports on overall DMARC pass/fails from receiving email servers and see if the organization email domain is being impersonated and/or make sure SPF, DKIM, and DMARC is configured correctly for all email senders in the sending domain.

**Figure 4. How DMARC Works with SPF and DKIM**



The receiving email server checks the sending domain's DMARC record published in DNS for guidance on how to handle incoming emails that fail SPF and/or DKIM checks. This is only a recommendation, as most email servers can override it based on their own configured policies (Reject, quarantine, mark as spam, etc.). These policies are typically specific to the receiving server.

**NOTE** Unless specifically overwritten on a given receiving email server, the sender's DMARC suggestion will typically be followed.



The resulting reports will show all the various sending IP addresses of email claiming to be from the sending organizations domain name, but that failed SPF and/or DKIM checks. Initially these could be valid email senders without properly configured SPF and/or DKIM records. After all of these are identified and corrected, this list will be IP addresses of systems sending email trying to impersonate the sending organization’s domain.

**NOTE** These reports will be managed and viewable in the MS-ISAC/EI-ISAC EPS system.

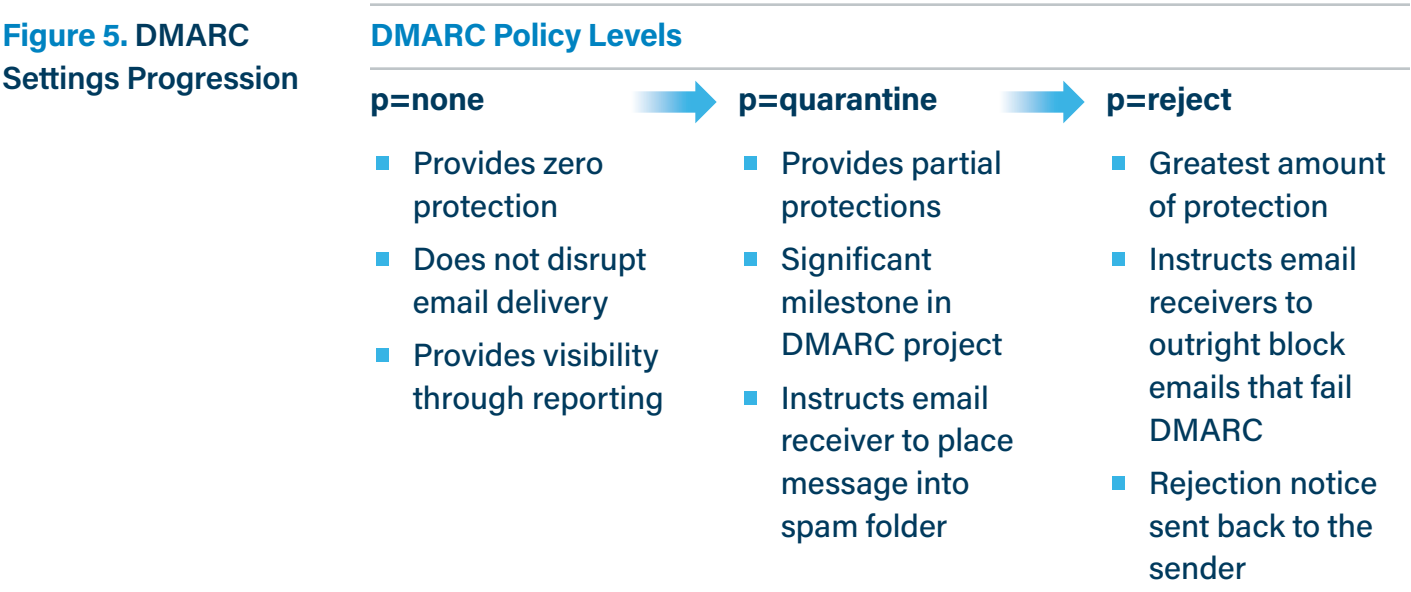
## How to Rollout DMARC

DMARC is a powerful security tool and if used indiscriminately it can cause problems. The following are some important configuration settings for DMARC.

<b>v</b>	The DMARC version being used. There’s only one version as of now, so it’s always v=DMARC1.
<b>p=none</b>	This is the first policy to be applied in a traditional DMARC rollout project. None is used as a means of gaining full visibility into how your domain is being used without impacting or influencing how your email is treated by email receivers. None provides zero protection but affords you the same visibility (DMARC reports) as the other, more restrictive policies (via DMARC reports).
<b>p=quarantine</b>	This is the second policy to be applied in a traditional DMARC rollout project. The “quarantine” policy provides partial protections against unauthorized use of your domain and represents a significant milestone in a DMARC project. “Quarantine” instructs the email receiver that they should still accept the message but downgrade the trustworthiness of the email and place it into the recipient’s spam/quarantine folder.
<b>p=reject</b>	This is the final policy to be applied in a traditional DMARC rollout project and provides the greatest amount of protection against unauthorized use of your domain. “Reject” instructs email receivers to outright block emails that fail the DMARC check. Unlike “Quarantine”, with “Reject” a message rejection notice is generated back to the sender. These blocking events are also made apparent in DMARC reports so you can readily observe how many messages are rejected and by what email source.

<b>pct</b>	<p>While the pct tag is optional in a DMARC record, by gradually increasing the percentage, you can discover necessary actions and address them before establishing a 100% “Quarantine” or “Reject” DMARC policy (typically finding valid email senders that are not yet properly configured with SPF and DKIM).</p> <p>If pct tag is not included in a DMARC record, 100% is the default value; tag values range from 1% to 100%. Because “None” is a monitoring policy with no action taken on email flows, the pct tag is superfluous and should not be used with “None”</p>
<b>fo</b>	<p>DMARC failure reporting options:</p> <p>fo=0 (Default): A DMARC failure/forensic report is sent if the email fails both SPF and DKIM alignment.</p> <p>fo=1: A DMARC failure/forensic report is sent to you when your email fails either SPF or DKIM alignment. This is the required setting for the MS-ISAC/EI-ISAC EPS system.</p>
<b>ruf</b>	<p>The email address where DMARC forensic ruf report is to be delivered. Specifying this tag implies that the owner requires recipient servers to send detailed reports on every message that fails DMARC validation. This is the required setting for the MS-ISAC/EI-ISAC EPS system.</p>
<b>rua</b>	<p>The email address or web server to which reporting organizations must deliver their DMARC aggregate rua data. This is the required setting for the MS-ISAC/EI-ISAC EPS system.</p>

In general, these settings (DMARC policy) are applied in sequence with a testing period in between to make sure everything is working as desired. Advancing the DMARC policy too soon, or without proper visibility, may result in blocked or degraded delivery of your legitimate email.



Initially the DMARC policy should be set to p=none and the resulting reports monitored and acted upon to make sure all valid email senders are properly configured with SPF and DKIM. Once confidence is high that all valid email servers have been identified and properly configured, the DMARC policy should be slowly progressed and reports monitored, following these suggestions (can be longer as needed):

Week 1	p=quarantine, pct=10	Week 6	p=reject, pct=10
Week 2	p=quarantine, pct=25	Week 7	p= reject, pct=25
Week 3	p=quarantine, pct=50	Week 8	p= reject, pct=50
Week 4	p=quarantine, pct=75	Week 9	p= reject, pct=75
Week 5	p=quarantine, pct=100	Week 10	p= reject, pct=100

**NOTE** When you advance the DMARC policies and increase pct tags, pay close attention to email flows (DMARC reports) to ensure that a high rate of DMARC compliance is achieved and maintained. Generally speaking, a DMARC compliance rate above 98% per domain is recommended.

# Google Workspace Configuration

To configure DMARC for your domain in Google Workspace, start by logging into both your Google Workspace admin panel (<https://admin.google.com>) and your domain registrar's, or DNS hosting service's, admin/control panel.

## DKIM Configuration

In your Google Workspace admin panel (<https://admin.google.com>) select from the left side menu tree:

- Apps, then
- Google Workspace, then
- Gmail
- From the right side set of options select
  - Authenticate Email

Now select Generate New Record and specify the Select DKIM key bit length (we recommend using 2048 where it is supported) and the Prefix selector. The Prefix selector defaults to Google and should only be changed if your organization has an existing DKIM key with the Prefix selector set to google. You will need to enter the resulting TXT record value into your domain registrar's admin/control panel to update the DNS record.

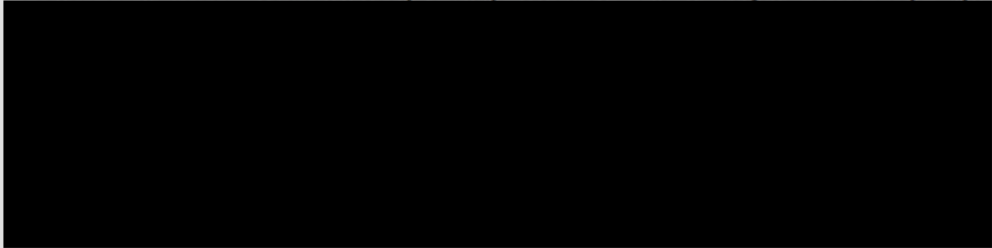
**Figure 6.** Exmample of a resulting DKIM key

DNS Host name (TXT record name):  
google.\_domainkey

TXT record value:

v=DKIM1; k=rsa;

p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIaKNWG  
YheM4wbEmkY+SXm50GngBAiuqFGJKKOzVa+JZkQIsE4rmA4fiFEgc



On the domain registrar's admin/control panel, go into the DNS settings for your domain and do the following:

- 1 Create a new custom record under the DNS settings and select the TXT type.
  - a Enter the DNS Host name (TXT record name) of the newly generated key (`google._domainkey` in the example above) into the name field for this new record (generally called Host or Hostname – domain registrar dependent).
  - b Then enter the TXT record value of the newly generated key into the content field (generally called Content or Data – domain registrar dependent).
  - c Save the new record.
- 2 Go back to the Google admin panel and select Start Authentication. This has enabled DKIM for your domain (if you have multiple domains, subdomains, follow the same steps for each one).

**NOTE** It may take up to 48 hours for DNS changes to fully propagate.

## Configure SPF in DNS Record

- 1 In the domain registrar's admin/control panel:
  - a Create another new record in the DNS settings of type TXT.
    - i Enter `@` into the hostname field and `v=spf1 include:_spf.google.com ~all` into the content field.
    - ii Save the new record.

## Configure DMARC in DNS Record

1 Create a third new record in the DNS settings of type TXT.

a Enter @ into the hostname field and `v=DMARC1; p=none; rua=mailto:report@domain1.com; ruf=mailto:report@domain1.com` into the content field.

i Make sure to replace the email address above (`report@domain1.com`) with a valid email address within your organization because every mail server that gets mail from your domain will send daily reports to that email address.

**NOTE** When using the MS-ISAC/EI-ISAC EPS, this string will be provided to you and will have the following basic form:

```
v=DMARC1; p=reject; rua=mailto:12ab34cd56ef.a@dmarcinput.com,mailto:dmarc_agg@vali.email,mailto:bef13fabf960531@rep.dmarcanalyzer.com; ruf=mailto: 12ab34cd56ef.f@dmarcinput.com,mailto:bef13fabf960531@for.dmarcanalyzer.com; fo=1; pct=100
```

- The email address (`12ab34cd56ef.a@dmarcinput.com`) will be replaced with something unique for your site.
- Please copy the string into the DNS record hostname field exactly as sent.

2 Save the new record.

A staged approach is recommended when configuring DMARC records in DNS. The first stage will involve setting the DMARC policy to `p=none` and then analyze the reports to identify any false positives or misconfigurations that need to be addressed. Over time the goal is to move to the policy to `p=quarantine` and then `p=reject` with `pct=100` defined. For more information on this process please review Item 3 (Information on [Advancing your DMARC Policy](#)) in the Additional Information section below.

**NOTE** It may take up to 48 hours for DNS changes to fully propagate.

## Additional Information

- Additional information about DMARC, DKIM, and SPF setup can be found in [Google Workspace Documentation](#).
- [DMARC RUA and RUF Reports](#)
- [Advancing your DMARC Policy](#)
- [Common DMARC Record Errors](#)
- [DMARC Failure Reporting Options](#)

# Microsoft 365 Configuration

To configure DMARC for your domain in Google Workspace, start by logging into both your Microsoft 365 admin panel and your domain registrar's, or DNS hosting service's, admin/control panel.

## Configure DKIM in Microsoft 365

DKIM is configured in two stages. First, the necessary DNS records need to be created. This is done either in the control panel at domain registrar or a DNS hosting service. Often the same company. The second stage involves enabling message signing for the domain(s) in the Microsoft Defender admin center.

### Configure DKIM in DNS Records

Two new custom records are required.

- 1 Create a new custom record under the DNS settings and select the CNAME type.
  - a Enter `selector1._domainkey` into the name field for this new record (generally called Host or Hostname – domain registrar dependent).
  - b Then enter `selector1-<CustomDomain>._domainkey.<InitialDomain>` into the content field (generally called Content or Data – domain registrar dependent).
    - i The data field can be constructed by replacing `<CustomDomain>` with the custom domain name but with the periods replaced by dashes. For example, `domain1.com` becomes `domain1-com`
    - ii `<InitialDomain>` is the `*.onmicrosoft.com` domain that was created for you when you initially set up your tenant, i.e. `<random>.onmicrosoft.com`
    - iii Assuming your domain is `domain1.com` and `*.onmicrosoft.com` created for you was `abcde.onmicrosoft.com` the resulting data entries would look like the following:
      - `selector1-domain1-com._domainkey.abcde.onmicrosoft.com`
  - c Save the new record.
- 2 Create another new custom record under the DNS settings and select the CNAME type.
  - a Enter `selector2._domainkey` into the name field for this new record (generally called Host or Hostname – domain registrar dependent).
  - b Then enter `selector2-<CustomDomain>._domainkey.<InitialDomain>` into the content field (generally called Content or Data – domain registrar dependent).



- i The data field can be constructed by replacing `<CustomDomain>` with the custom domain name but with the periods replaced by dashes. For example, domain1.com becomes domain1-com
  - ii `<InitialDomain>` is the `*.onmicrosoft.com` domain that was created for you when you initially set up your tenant, i.e. `<random>.onmicrosoft.com`
  - iii Assuming your domain is domain1.com and `*.onmicrosoft.com` created for you was `abcde.onmicrosoft.com` the resulting data entries would look like the following:
    - `selector2-domain1-com._domainkey.abcde.onmicrosoft.com`
- c Save the new record.

**NOTE** It may take up to 48 hours for DNS changes to fully propagate.

Repeat the steps above for any additional domains or subdomains sending outbound email.

## Configure DKIM Signing of Messages in Microsoft Defender

It can take time for DNS records to fully publish and replicate, so only proceed to the next steps after waiting for several minutes.

- 1 Access the DKIM portion of the Defender portal at <https://security.microsoft.com/authentication?viewid=DKIM> and for each domain and subdomain in the list, perform the following:
  - a Select a domain or subdomain.
  - b Below **Sign messages for this domain with DKIM signatures** click **Enable**.
  - c The DKIM CNAME records created earlier will then be discovered and a confirmation dialog box will open.
  - d Repeat the steps for additional domains or subdomains as needed.

## Configure SPF in DNS Record

Configuring an SPF record is a prerequisite during the initial setup of a custom domain with Microsoft 365, so it is entirely likely one already exists for at least one domain. It is important to validate that configuration has not drifted and still is in compliance. It is also important to configure an SPF record for each domain owned, including any subdomains.

SPF is configured at the domain registrar or DNS hosting service (often the same company, but DNS records can also be hosted and modified elsewhere).

- 1 Create another new custom record under the DNS settings and select the TXT type.
  - a Enter `@` into the hostname field and `v=spf1 include:spf.protection.outlook.com -all` into the content field.
  - b Save the new record.

## Configure DMARC in DNS Record

- 1 Create a third new record in the DNS settings of type TXT.
  - a Enter `_dmarc` into the hostname field and `v=DMARC1; p=none; rua=mailto:report@domain1.com; ruf=mailto:report@domain1.com` into the content field.
  - i Make sure to replace the email address above (`report@domain1.com`) with a valid email address within your organization because every mail server that gets mail from your domain will send daily reports to that email address.

**NOTE** When using the MS-ISAC/EI-ISAC EPS, this string will be provided to you and will have the following basic form:

```
v=DMARC1; p=reject; rua=mailto:12ab34cd56ef.a@dmarcinput.com,mailto:dmarc_agg@vali.email,mailto:bef13fabf960531@rep.dmarcanalyzer.com; ruf=mailto: 12ab34cd56ef.f@dmarcinput.com,mailto:bef13fabf960531@for.dmarcanalyzer.com; fo=1; pct=100
```

- ❑ The email address (`12ab34cd56ef.a@dmarcinput.com`) will be replaced with something unique for your site.
- ❑ Please copy the string into the DNS record hostname field exactly as sent.

- 2 Save the new record.

A staged approach is recommended when configuring DMARC records in DNS. The first stage will involve setting the DMARC policy to `p=none` and then analyze the reports to identify any false positives or misconfigurations that need to be addressed. Over time, the goal is to move to the policy to `p=quarantine` and then `p=reject` with `pct=100` defined. For more information on this process, please review Item 3 (Information on [Advancing your DMARC Policy](#)) in the Additional Information section below.

**NOTE** By default, when `pct` is left undefined 100 percent of email is impacted. By defining `pct=100` we are being implicit and ensuring no other value on the flag `pct` is being used.

**NOTE** It may take up to 48 hours for DNS changes to fully propagate.

## DMARC for the MOERA Domain

The Microsoft Online Email Routing Address (MOERA) domain is created by default for each tenant when you sign up for the service. The domain name is unique and formatted like `*.onmicrosoft.com`. Given that it can be used for sending outbound email, it should have a related DMARC TXT record configured.

This record is configured from the Microsoft 365 Admin Center and not your domain registrar.

- 1 Navigate to <https://admin.microsoft.com/Adminportal/Home#/Domains>
- 2 On the **Domains** page select your unique `*.onmicrosoft.com` domain by clicking on the domain name itself.
- 3 Select DNS records and click **Add record**.
- 4 Fill out the fields on the right-side flyout as shown in the following table:

Type	TXT
TXT name	<code>_dmarc</code>
TXT value	<code>v=DMARC1; p=reject; pct=100; rua=mailto:report@domain1.com; ruf=mailto:report@domain1.com</code>  Make sure to replace the email address above ( <code>report@domain1.com</code> ) with a valid email address within your organization because every mail server that gets mail from your domain will send daily reports to that email address.  <b>NOTE</b> When using the MS-ISAC/EI-ISAC EPS, this string will be provided to you and will have the following basic form:  <code>v=DMARC1; p=reject; rua=mailto:12ab34cd56ef.a@dmarcinput.com, mailto:dmarc_agg@vali.email, mailto:bef13fabf960531@rep.dmarcanalyzer.com; ruf=mailto:12ab34cd56ef.f@dmarcinput.com, mailto:bef13fabf960531@for.dmarcanalyzer.com; fo=1; pct=100</code>  The email address ( <code>12ab34cd56ef.a@dmarcinput.com</code> ) will be replaced with something unique for your site.  Please copy the string into the DNS record hostname field exactly as sent.
TTL	1 hour

- 5 Click **Save**.

A staged approach is recommended when configuring DMARC records in DNS. The first stage will involve setting the DMARC policy to **p=none** and then analyzing the reports to identify any false positives or misconfigurations that need to be addressed. After no more than two weeks, move to an actionable policy **p=quarantine** or **p=reject**, which should be adopted with **pct=100** defined.

**NOTE** By default, when pct is left undefined, 100 percent of email is impacted. By defining **pct=100** we are being implicit and ensuring no other value on the flag pct is being used.

## Additional Information

- Information about DMARC, DKIM, and SPF setup can be found in [Microsoft 365 Documentation](#).
- [DMARC RUA and RUF Reports](#)
- [Advancing your DMARC Policy](#)
- [Common DMARC Record Errors](#)
- [DMARC Failure Reporting Options](#)

# Conclusion

Implementing DMARC is an important email security step. Cybercriminals are much more likely to give up on trying to spoof a domain if they see properly configured DMARC records in the domain's DNS. Receiving servers also know that emails coming from DMARC secured domains are much more likely to be legitimate.

As a reminder, administrators can ease into using DMARC. They can start with a "none" policy and observe what happens. This basically means that your emails will be going through the relevant checks on the receiving side. If they fail, it will be reported but it won't influence the email deliverability. The resulting MS-ISAC/EI-ISAC EPS DMARC reports will have useful data covering authentication issues. Using these reports, administrators can quickly identify if someone is trying to spoof the domain

# Appendix

## Third-party Email Providers

**NOTE** Details on this subject are out of scope for this basic guide, but this section gives an overview of what to be aware of.

Configuring an email system on Microsoft 365 and/or Google Workspace is straight forward and documented in this guide. It is also possible that an organization is using some other third-party email provider to send email on their behalf. Some examples include:

- **Microsoft SharePoint:** This product can send email to people when a page gets updated, and this email can look like that came from the owner's organization.
- **Marketing Campaigns:** An organization may use an email marketing firm (Constant Contact, etc.) to send out mass emails that look like they came from the original client organization.

The issue with these systems is that they are essentially impersonating the sender's domain, but legitimately so (they are approved to do this). In the end, anyone setting up DMARC on these systems will need to determine the following:

- **Do they use third-party email senders?**
  - Monitoring the DMARC logs will assist here. Find senders that are failing DMARC and determine if they are legitimate third parties or not.
- **Once a valid third-party sender is discovered, work with that vendor to properly configure DMARC compatibility.**
  - Every sender is different so the vendor needs to be contacted to determine the details of the configuration. Since DMARC is becoming more widely used, and a requirement by some providers (Google and Yahoo), most reputable third-party senders now support DMARC and information on DMARC configuration can be found on their websites.
  - A guide to help determine if a given provider's DMARC support is here: [DMARC-Related email sources](#)

## Additional Information

- [StackOverflow thread on third-party email providers](#)
- [Mimecast post on third-party email providers](#)
- [How to ask your vendor to send DMARC-compliant email on your behalf](#)

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.



 [www.cisecurity.org](http://www.cisecurity.org)

 [info@cisecurity.org](mailto:info@cisecurity.org)

 518-266-3460

 Center for Internet Security

 CenterforIntSec

 @CISecurity

 TheCISecurity

 cisecurity