



SPF, DKIM, DMARC Setup Guide

for Google Workspace



Introduction

Google Workspace, formerly known as G Suite, is Google's cloud computing platform that offers productivity and work collaboration tools. If you've not been living under a rock, you might know at least a few of the products — Google Slides, Docs, Sheets, Calendar, and others. For proper DMARC setup, you need to first configure SPF and DKIM.

SPF Records allow receiving servers to check whether an email with the specified source domain was actually sent from a server authorized by the owner of this domain. The DKIM adds a digital signature to each message. This allows the receiving server to check if the message has been falsified or changed in transmission.

In this PDF, We'll be discussing how to authenticate SPF and DKIM on your Google Workspace and how to setup DMARC.

TABLE OF CONTENTS

Cover.....	1
Introduction.....	2
<u>How to setup SPF Record.....</u>	<u>4</u>
<u>Configuring DKIM for GSuite.....</u>	<u>6</u>
<u>DMARC Setup for Google Workspace.....</u>	<u>9</u>
<u>Feedback.....</u>	<u>11</u>

How to setup SPF Record

In order to authorize Google to send emails on your domain's behalf, you will need to create or update your SPF record, which includes the following mechanism:

include:_spf.google.com

You can achieve this easily with our SPF Record Generator tool; here are the steps:



STEP 1

Generate a new SPF Record by authorizing Google

The screenshot shows the 'SPF Record Generator' web interface. It has a title 'SPF Record Generator' and a subtitle 'Use this tool to generate your SPF record.' Below this are several input fields and radio buttons. The 'mx' field has radio buttons for 'Yes (recommended)' (selected) and 'No'. The 'a' field also has radio buttons for 'Yes (recommended)' (selected) and 'No'. The 'ip4:___' field contains 'e.g. 10.0.0.1/20 192.168.0.10'. The 'ip6:___' field contains 'e.g. 2001:db8:0:1:1:1:1:1 2404:6800:4000::/36'. The 'a:___' field contains 'e.g. example2.com'. The 'include:___' field contains '_spf.google.com'. The 'Policy' dropdown is set to 'SoftFail (Not compliant will be accepted but marked)'. A red arrow points to a blue button labeled 'Generate SPF Record'.



STEP 2

Copy the newly generated SPF Record



STEP 3

Update your DNS TXT Record for SPF at your DNS provider (We will show examples with GoDaddy and Cloudflare)

Ex. GoDaddy

The screenshot shows the GoDaddy DNS management interface. It features a form with the following fields:

- Type**: A dropdown menu set to "TXT".
- Host**: A text input field containing "@".
- TXT Value**: A text input field containing "v=spf1 include:_spf.google.com".
- TTL**: A dropdown menu set to "1 Hour".
- Buttons**: "Save" and "Cancel" buttons at the bottom right.

Ex. Cloudflare

The screenshot shows the Cloudflare DNS management interface. It features a form with the following fields:

- Type**: A dropdown menu set to "TXT".
- Name**: A text input field containing "@".
- TTL**: A dropdown menu set to "Auto".
- Content**: A text input field containing "v=spf1 include:_spf.google.com ~all".
- Buttons**: "Cancel" and "Save" buttons at the bottom right.

Click save.

Important Note: Make sure you don't create multiple SPF TXT records on one domain. If you do, SPF will return a PermError.

If you're using multiple IPs, ESPs, and third-party services for your various email strategies, you should include them in a single SPF Record.

E.g `v=spf1 ip4:17.67.137.221 include:_spf.google.com include:thirdpartyservice.com ~all`

Configuring DKIM for GSuite



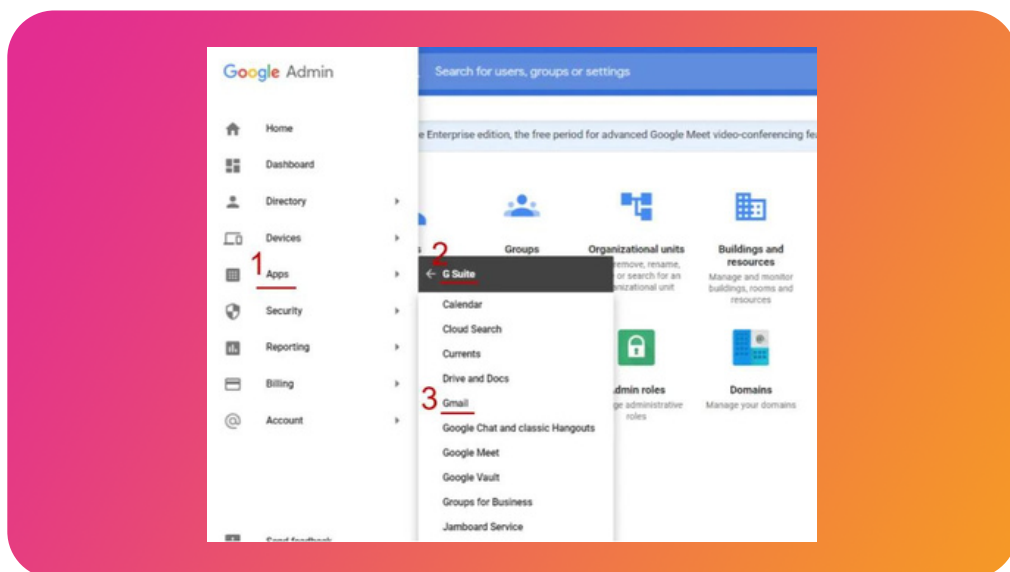
STEP 1

In the Google Admin Console (at admin.google.com)



STEP 2

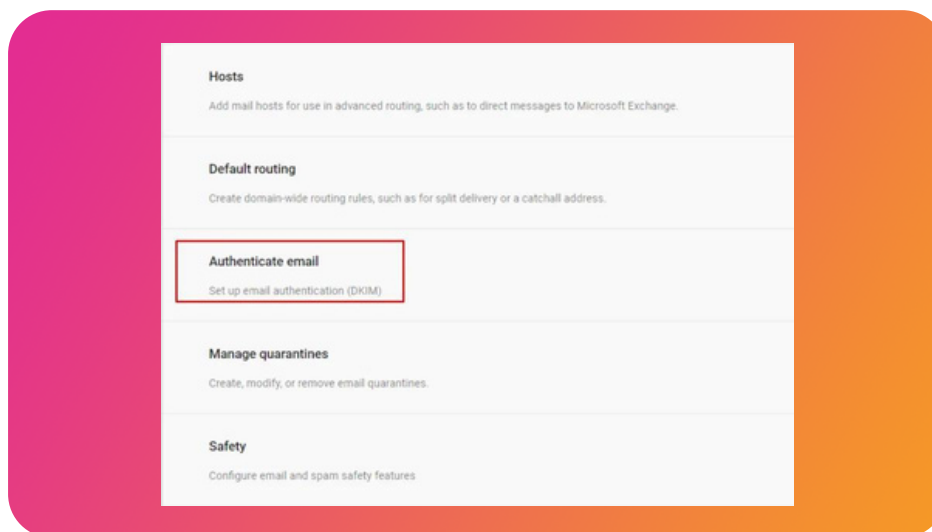
Open Apps > G Suite > Gmail





STEP 3

Click 'Authenticate Email'



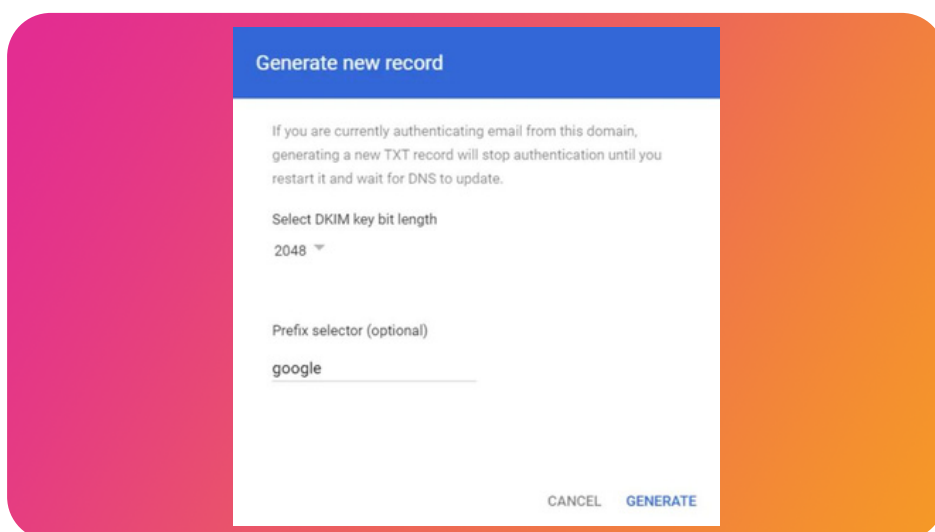
STEP 4

By default, your main domain is selected. Click on the primary domain name or select another domain where DKIM will be used.



STEP 5

Click "Generate New Record". GSuite DKIM Public Key will be generated for your domain – copy these values.





STEP 6

Publish the provided TXT Record into your DNS

[selector]_domainkey.yourdomain.com – in this case, google._domainkey.yourdomain.com.

Ex. GoDaddy

The screenshot shows the GoDaddy DNS management interface. It features a form with the following fields:

- Type:** A dropdown menu set to "TXT".
- Host:** A text input field containing "google._domainkey".
- TXT Value:** A text input field containing "v=DKIM1; k=rsa; p=MIGfMA0G".
- TTL:** A dropdown menu set to "1 Hour".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

Ex. Cloudflare

The screenshot shows the Cloudflare DNS management interface. It features a form with the following fields:

- Type:** A dropdown menu set to "TXT".
- Name:** A text input field containing "google._domainkey".
- TTL:** A dropdown menu set to "Auto".
- Content:** A text area containing "v=DKIM1; k=rsa; p=MIGfMA0GCSq".
- Buttons:** "Cancel" and "Save" buttons at the bottom right.



STEP 7

Go to the administrator console and click the 'Start Authentication', and you're all set!

DMARC Setup for Google Workspace

Now that you're done with SPF and DKIM configurations, let's learn how to setup DMARC for your Google Workspace.

To setup DMARC, first, generate the record for your domain — go to EasyDMARC's DMARC record generator page and create it.

The screenshot shows the 'DMARC Generator' tab in the EasyDMARC interface. The 'DMARC Record Generator' section includes the following fields and options:

- Policy type ***: Radio buttons for ☒ None (monitoring), ☐ Quarantine, and ☐ Reject.
- Aggregate reporting ***: Text input field containing 'mailto:example@easydmarc.com'.
- Subdomain policy type**: Dropdown menu with '-----' selected.
- SPF identifier alignment**: Dropdown menu with '-----' selected.
- DKIM identifier alignment**: Dropdown menu with '-----' selected.
- Percentage applied to**: Text input field.
- Reporting interval**: Text input field.
- Failure reporting**: Text input field containing 'mailto:example@easydmarc.com'.
- Failure reporting options**: Checkboxes for ☐ 0, ☒ 1, ☐ d, and ☐ s.

A blue button labeled 'Generate DMARC Record' is located at the bottom of the form.

Publish the generated txt record in your DNS. You will start receiving DMARC XML reports within 48 hours.

EasyDMARC will analyze your DMARC reports and give you suggestions, alerts, and configuration instructions. We also have a comprehensive guide on how to implement DMARC on EasyDMARC.

Your email system is now secure!

Implementing SPF, DKIM, and DMARC is more than a technical task; it's an investment in the security and integrity of your email communications. Following this guide will not only enhance your email deliverability but build trust with your recipients! As technology evolves, staying ahead with these protocols is crucial in maintaining a robust defense against increasingly sophisticated email threats.

About SmartSaaS

SmartSaaS is a global e-learning company specializing in pre-revenue to growth stage SaaS startups. Our bootcamps, sales models, and guides cover today's leading SaaS strategies and roadmaps proven to drive consistent scalable revenue growth.

With over 40 years of collective SaaS, sales and executive experience at early to growth stage startups, SmartSaaS delivers the right advice specific to companies just getting started to reaching \$50M in ARR.