

# Updating DNS , SPF , DKIM, and DMARC

There are 3 settings that needs to updated or check

## 1) SPF

- Type: Text
- Name : @
- TXT Value : v=spf1 include:\_spf.google.com ~all ( For GSuite users)
- TXT Value : v=spf1 include:\_spf.outlook.com ~all (For Outlook users)

If you are using more than one mail server to send mails then append the other mail server name as well

Example we sometimes use Sendgrid to send notifications to users but use Gsuite for regular emails.

WIn such case our SPF TXT Value is:

TXT Value : v=spf1 include:\_spf.google.com include:sendgrid.net ~all

- TTL:600

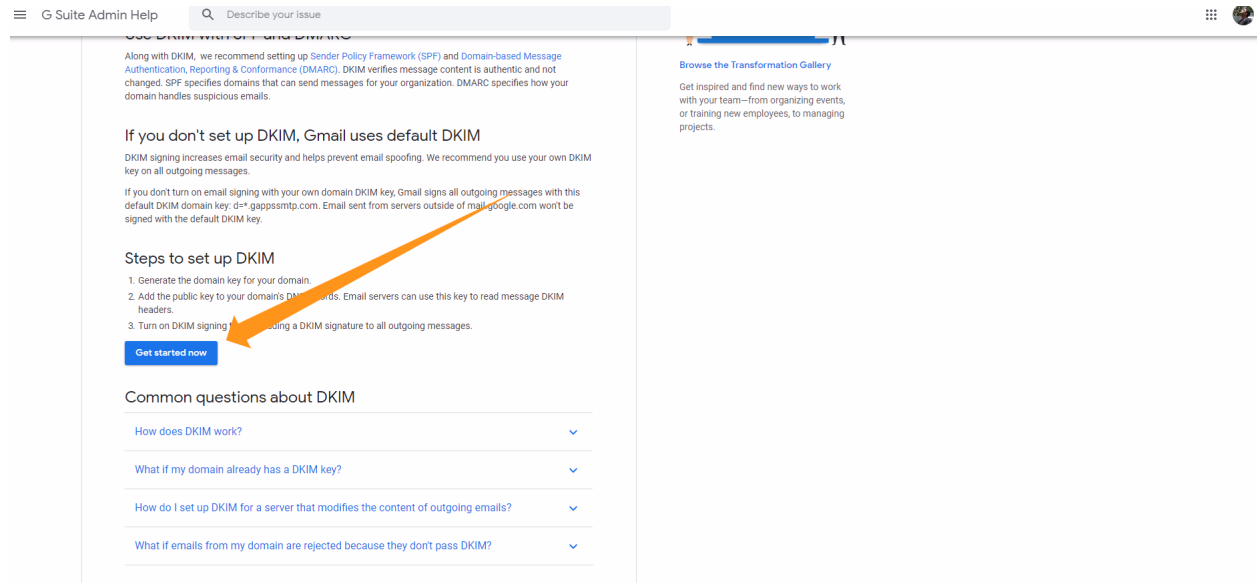
**Important** : Please ensure that there's only one SPF record.

## 2) DKIM

For G Suite users:

To set up DKIM Please follow the instruction here

<https://support.google.com/a/answer/174124?hl=en>



## For Outlook users:

1. Log in to your DNS. ...
2. Go to Advanced DNS Management. ...
3. You will need to publish a new TEXT (TXT) record for DKIM. ...
4. The DKIM record will require publishing a selector record. ...
5. [Optional] If possible, adjust the TTL to something like 60, so it will propagate faster.

## Article to help clarify things

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-dkim-to-validate-outbound-email>

## 3) DMARC

This remains standard for all Outlook, Gmail, Yahoo email service providers.

Step 1: Please sign up for a free account at <https://www.dmarcanalyzer.com/>

Step 2: You get a free account for 14 days, with 1 Domain that you can monitor for abuse ( if someone has reported the domain for abuse ) for example we check for alore.io

The screenshot shows the 'Setup wizard - Add domain(s)' screen in the DMARCAnalyzer interface. The left sidebar has a menu with 'DNS records' highlighted. An orange arrow points from the 'DNS records' menu item to the 'Add domain(s)' option. The main content area has a progress bar with three steps, the first of which is active. Below the progress bar, there is a section titled 'Enter your domain to start the DMARC setup'. This section contains a text input field with 'mydomain.com' and a 'Next' button. An orange arrow points from the text 'Enter Domain name' to the input field. The top of the interface shows the user's name 'Vikas' and a trial period expiration notice.

DMARCAnalyzer

Vikas 49,207.52,254

Your trial period has expired! Upgrade now

1% 254 / 25,000

Upgrade now

MAIN

- Guide
- Domains
- DMARC aggregate reports
- DMARC forensic reports
- Timeline
- DNS records**
- Add domain(s)
- DMARC record generator
- DMARC setup wizard
- SPF Record Check
- DKIM Record Check
- DMARC Record Check
- Alerts & Reporting
- Knowledgebase

Setup wizard - Add domain(s)

1 2 3

Enter your domain to start the DMARC setup

This setup guide will guide you through the process of creating your own DMARC DNS record. A DMARC record is the core of each DMARC deployment project, have you define the DMARC record rule sets. After placing the DMARC record into your DNS record you will start collecting valuable DMARC data. With this data you will gain insight in your email channel(s). By using this data you can gain a better understanding of your mail streams, ensure that the various IPs sending email claiming to come from your domain are indeed legitimate, configure them properly with DKIM or add them to their SPF range. Then you can start validating policies for Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). All three policies together will get you a stronger email authentication mechanism.

Let's start with generating a DMARC record for your domain.

Enter the domain you want to manage and we will guide you through the steps to protect it.

mydomain.com

Next

Enter Domain name

?

The screenshot shows the 'Create your own DMARC record' screen in the DMARCAnalyzer interface. The left sidebar has a menu with 'DNS records' highlighted. An orange arrow points from the 'DNS records' menu item to the 'Add domain(s)' option. The main content area has a progress bar with three steps, the second of which is active. Below the progress bar, there is a section titled 'Create your own DMARC record'. This section contains a text input field with 'Quarantine' and a 'Next' button. An orange arrow points from the text 'Would you like to use a different policy for your subdomains?' to the 'No' radio button. The top of the interface shows the user's name 'Vikas' and a trial period expiration notice.

DMARCAnalyzer

Vikas 49,207.52,254

Your trial period has expired! Upgrade now

1% 254 / 25,000

Upgrade now

MAIN

- Guide
- Domains
- DMARC aggregate reports
- DMARC forensic reports
- Timeline
- DNS records**
- Add domain(s)
- DMARC record generator
- DMARC setup wizard
- SPF Record Check
- DKIM Record Check
- DMARC Record Check
- Alerts & Reporting
- Knowledgebase

Create your own DMARC record

In this step we are going to define the rule sets of your DMARC record. The DMARC record tells ISP's who adopted DMARC how they should handle your emails and optionally where to send the DMARC reports.

Select the policy level of your DMARC project

A DMARC policy tells email receivers like Microsoft (Hotmail, Live, Outlook etc), Gmail, Yahoo! and other Internet Service Providers who adopted DMARC how to handle email that fails the DMARC check. In other words, a DMARC policy influences the way email is handled. There are three DMARC policies which you can add to your DMARC record. Depending on the DMARC policy, emails that fail the DMARC check will be handled differently. There are three policies to choose from: none, quarantine or reject. We recommend to start off with the monitor policy (none).

Select your DMARC policy

Quarantine

With the DMARC policy quarantine, Internet Service Providers who've DMARC will put emails failing the DMARC check in special 'quarantine' folders like the junk or spam folder. This DMARC policy influences the way email is handled, however failing emails will still arrive.

Would you like to use a different policy for your subdomains?

☒ No ☐ Yes

Advanced options

Next

?

**DMARC Analyzer**

1% 250 / 25000

**Upgrade now**

**MAIN**

- Guides
- Domains
- DMARC aggregate reports
- DMARC forensic reports
- Timeline
- DNS records**
  - Add domains
  - DMARC record generator
  - DMARC setup wizard
  - SPF Record Check
  - DKIM Record Check
  - DMARC Record Check
- Alerts & Reporting
- Knowledgebase

**Publish your DMARC record into your DNS**

You have created your own DMARC record! In order to start collecting DMARC data, you will need to publish it into your DNS. This way DMARC Analyzer starts receiving DMARC reports for you. You will then see valuable DMARC data dripping into your account.

To start collecting DMARC data you need to publish the following DMARC record into your DNS record:

We have some setup guides based on frequently used registrars. Please select a registrar below to open the guide [click here to view our default guide](#).

Select a registrar to view its setup guide

| Selector | Type | Value / Data / Points to                                                                                                 |
|----------|------|--------------------------------------------------------------------------------------------------------------------------|
| _dmarc   | TXT  | v=DMARC1; p=quarantine; rua=mailto:ca334c16b355057@rep.dmarcanalyzer.com; ruf=mailto:email@yourdomain.com; pct=100; fo=1 |

**Enter this TXT record @godaddy**

**Complete Setup and test it**

**Complete setup**

**Multiple domains?**

If you have multiple domains which you would like to analyze, simply add this DNS record to those domains. Too directly bulk add these domains [click here](#)

After all this is done

Please go this domain <https://mxtoolbox.com/domain>

Eg. enter your email domain at <https://mxtoolbox.com/domain/>

If you get errors in red, these need to be removed.

**I-MIDASTOUCH.COM Domain Health Report**

Complete

| Problems   | Blacklist  | Mail Server | Web Server | DNS       |
|------------|------------|-------------|------------|-----------|
| 2 Errors   | 0 Errors   | 2 Errors    | 0 Errors   | 0 Errors  |
| 10 Warning | 0 Warning  | 9 Warning   | 0 Warning  | 1 Warning |
| 585 Passed | 521 Passed | 45 Passed   | 3 Passed   | 16 Passed |

**12 Problems**

| Category | Host             | Result                                     |
|----------|------------------|--------------------------------------------|
| mx       | i-midastouch.com | No DMARC Record found                      |
| dmarc    | i-midastouch.com | DNS Record not found                       |
| dns      | i-midastouch.com | SOA Expire Value out of recommended range  |
| mx       | i-midastouch.com | DMARC Quarantine/Reject policy not enabled |

Feedback Contact Terms & Conditions Site Map API Privacy

Your IP is: 222.222.12.121

Phone: (888) 462-4652 | [feedback@mxtoolbox.com](mailto:feedback@mxtoolbox.com)

© Copyright 2004-2019, MXToolBox, Inc. All rights reserved.

Type here to search

ENG 2:56 PM 7/23/2019

This is the existing record.

The ones in red should turn green.

Ideally, it won't take more than 5 mins for records to update