Email Notification Security and Authentication

Download the PDF of this article.

In this Article

Related Articles

Email Notification Security and Authentication

FormAssembly adheres to common best practices when sending emails including:

1. Using consistent IP addresses when sending bulk emails
2. Keeping valid reverse DNS records for our mailing IP addresses
3. Using the same address in our email headers

To help improve the security of email messages sent from FormAssembly, we support the following options:

SPF Record

- FormAssembly requires all custom domains configured in sender emails to have an SPF record to verify and use that email for notifications.
- Any sender email from a domain without an SPF record for FormAssembly will default to no-reply@formassembly.com until verified.

If you are having email deliverability issues with our notifications or auto-responder emails, you should contact your IT/server administrator and ask them to publish or edit an existing SPF record to include FormAssembly as a supported host.

When generating this SPF record they will need to add the following:

```
include:spf1.formassembly.com
```

Note: DNS updates can take up to 48 hours to propagate. If an SPF record is recently configured, and verification of an email is attempted within this propagation window, the email verification may still fail. Please wait and try again.

If you continue to have additional email deliverability issues, please let our Support team know and we will be happy to assist you!

DKIM

DKIM can be set up for **Essentials plans and above**.

Please reach out to Support if you would like to have DKIM set up for your instance. The setup process may require 1-2 days to complete.

With your support request, you will need to provide the following:

1. Your instance URL
2. The email domain for which you are requesting DKIM setup
3. The DKIM selector name that you would like to use
    - **Note**: The DKIM selector name must be a single alphanumeric string (ex: mydkim1) with no special characters.

When setting up DKIM, it is recommended that you review the following FormAssembly Admin Dashboard settings:

- **Admin Dashboard | Settings | General (Administrator)** - Support Email and Bounce Email
- **Admin Dashboard | Settings | Miscellaneous (Notification Settings)** - Default Notification Email and Default Notification Sender

> **Note:** While there is no FormAssembly requirement for configuring DKIM, If your domain meets Google's definition of a "bulk sender" (you send more than 5,000 emails per day from your domain) and does not have DKIM, you could experience deliverability issues with your emails.

DMARC

DMARC setup should be possible once an SPF record and DKIM have been configured for your **Essentials plans and above**.

Gmail Sender Guideline Update FAQ

What is the Gmail Sender Guideline Update?

- Google will enforce specific guidelines for **all email senders** beginning **February 1st, 2024**. SPF (Sender Policy Framework) will be required on all Gmail-hosted domains, and both SPF and DKIM (DomainKeys Identified Mail) will be required for all domains that send more than 5,000 emails a day.
- These new requirements are an added security measure to prevent spam and ensure successful delivery without Google needing to limit sending rates.

My organization's email sender domain is not hosted by Gmail, does this still impact me?

- Yes, Google's update will impact emails sent to and from Gmail inboxes. Gmail is the most popular email client globally, so it's likely that your audiences will include Gmail addresses.
- If your organization does not meet Google's requirements, you may see impacts to your deliverability,

including your emails being sent to spam folders.

What actions are required with this update?

- **Required:** If you have configured any emails sent through FormAssembly to use a custom email domain, you must set up an SPF record to include FormAssembly as a supported host. Please see the section above on setting up SPF records.
- **Optional:** If you send more than 5,000 emails per day from your domain, including those sent through FormAssembly with a custom sender configuration, consider configuring DKIM. Visit the section above for information on DKIM setup in FormAssembly.

What impacts will you see with this change?

- SPF Required
  - Starting in February, FormAssembly will require all custom domains configured in sender emails to have an SPF record to verify and use that email for notifications.
  - Any sender email from a domain without an SPF record for FormAssembly will default to no-reply@formassembly.com until verified.
- DKIM Suggested
  - There will be no requirement for DKIM setup, but if your domain meets Google's definition of a "bulk sender" and does not have DKIM, you could experience deliverability issues with your emails.
  - You may want to discuss Google's updated guidelines with your email or marketing operations team.