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 for email messages sent from FormAssembly, we support the following options:

SPF Record

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:

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

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 **Enterprise Cloud and Compliance Cloud** accounts.

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 your EC/CC instance URL, the email domain for which you are requesting DKIM setup as well as the DKIM selector name (which must be a single alphanumeric string ex: mydkim1, no special characters) that you would like to use.

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

---

DMARC

DMARC setup should be possible once an SPF record and DKIM have been configured for your **Enterprise Cloud or Compliance Cloud** account.