

Set Up DKIM & SPF Records

Configuring your domain with DKIM & SPF Records enables the use of a custom **From Email** address in Alchemer [Email Actions](#) and [Email Campaigns](#).

If you prefer to send via a **SMTP** server, visit the instructions [here](#).

There are two DNS-based records that need to be in place (*though both records are of the same type (txt), two separate records are needed*):

- SPF record
- DKIM record

The setup process involves configuration both within Alchemer and on the domain's DNS record.

In order to configure your **DKIM** and **SPF** records, you will need to be an Alchemer Account Administrator. You will also likely need access to your organization's (or client's) domain administrator or IT Team (or direct access to your domain's DNS record settings).

Alchemer-Side Configuration

At this time Alchemer supports SPF/DKIM setups with a domain only (*www.example.com*) and does **not** support subdomain (*email.example.com*) builds.

To begin your DKIM/SPF configuration within Alchemer, follow these steps:

1. Navigate to your account integrations page via **Integrations > Data connectors** on the left hand navigation menu.
2. Scroll to the bottom-half of the **Integrations** page and click the **Configure** button next to the **Custom Email Settings** option.
3. Provide an **Integration Name**. This is the internal title that will be used to identify this integration in Email Actions and Email Campaigns. It is important to make this name something meaningful like *DKIM & SPF for alchemer.com*.
4. (Optional) Determine whether you want this integration to serve as the default for any Email Actions and Email Campaigns that are created going forward.

The option to **Use this integration as the default for all new email invitations and email actions** will be automatically selected. Un-check the option if needed.

5. Select **Send emails using Alchemer's servers (Setup SPF and DKIM)**. This will expose additional

fields for configuring this integration.

6. Within the **From Address** section, provide your **Domain Name** and **Default From Address**.

This is the domain that you want to use as your From Address within **Email Actions** and **Email Campaigns**. The above Default From Address can be updated when configuring your Email Actions or Campaigns (the domain cannot be updated).

Use this integration as the default for all new email invitations and email actions

Send emails using SurveyGizmo's servers (Setup SPF and DKIM)

Send emails using your own server (Setup SMTP)

From Address

This is the domain you want to use in your From addresses.

Domain Name

Default From Address

The next several steps will need to be executed within the domain's DNS settings by referencing the **SPF Settings** section.

Domain-Side Configuration

1. Within Alchemer, the **SPF Settings** section provides users with the **SPF Entry** that will need to be added to the domain's SPF record. Copy the SPF Entry from the provided field in the custom email integration being created:

Integration Name

To enable using a "From" address in email actions and email campaigns other than a Alchemer account, you must either send from your own SMTP server or configure your domain with SPF and DKIM records.

Use this integration as the default for all new email invitations and email actions

Send emails using Alchemer's servers (Setup SPF and DKIM)

Send emails using your own server (Setup SMTP)

From Address

This is the domain you want to use in your From addresses.

Domain Name

Default From Address

SPF Settings

Add the following entry to your domain's SPF record.

SPF Entry

Not Validated — We will attempt to validate your settings when you save

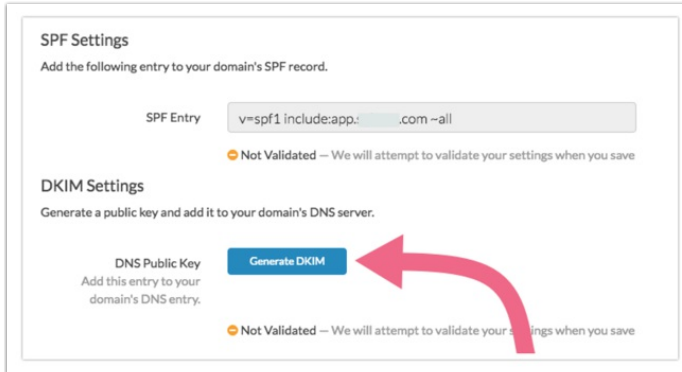
DKIM Settings

Generate a public key and add it to your domain's DNS server.

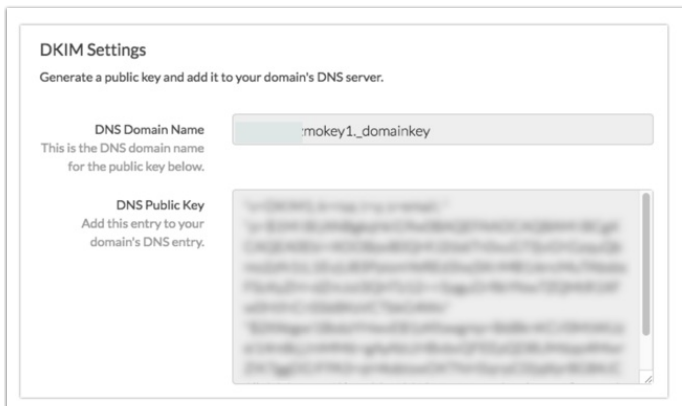
Within your domain's DNS settings, create a new TXT record and add the above content.

2. Back in Alchemer, under **DKIM Settings** you will need to generate your public key. This public key will then need to be added to your domain's DNS Server.

Click **Generate DKIM** to generate your public key.



A **DNS Domain Name** (the DNS domain name for the public key) as well as the **DNS Public Key** will be generated:



Within your domain's DNS settings, create a new TXT record with the following Name and Content:

- **Name:** `surveygizmokey1._domainkey.yourdomain.com`
- **Content:** paste the DNS Public Key you just generated

Important! Some systems require that you enter the quotes (that surround the key) and separate the public key into multiple strings under 255 characters whereas other systems for managing DNS do this automatically. This can cause extra quotes to be added to your key and make the DKIM record invalid. If your record is invalid, make sure that there are not multiple sets of quotes surrounding the key wherever it was entered.

3. Back in Alchemer, click the **Save** button to finish setup.

You will notice that both your SPF and DKIM Settings are not validated during setup. We will attempt to

validate your settings when you **Save** your integration. We perform this validation by sending a test email (to one of our servers) and reviewing the email headers of that test email.

Your DKIM & SPF Records will need to be verified before you can start using them in email sends. On the main **Integrations** page, look for the green check-mark under the **Verified** column.

Integrations			
Current Integrations	Name	Status	Verified
✉ DKIM/SPF Server (yourdomain.com)	DKIM & SPF for yourdomain.com	Active	✔
✉ DKIM/SPF Server (company.com)	DKIM & SPF for company.com	Testing	⊖
✉ DKIM/SPF Server (business.com)	DKIM & SPF for business.com	Disabled	⊖

The Test Link via *email campaigns* does **not** use DKIM/SPF information, and will **always** come from Alchemer. To test DKIM/SPF, send a live email campaign to the email of choice.

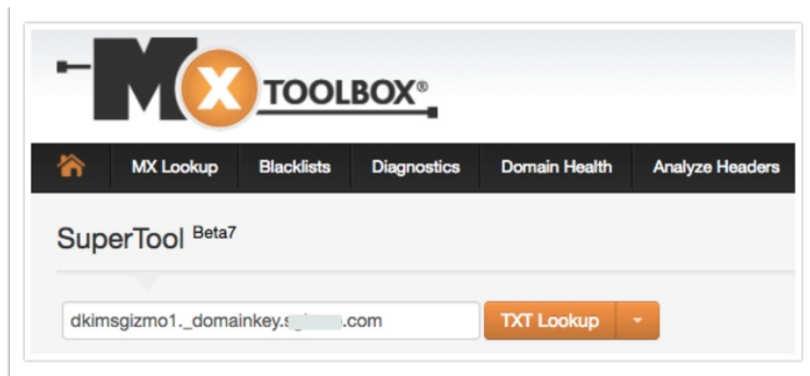
Testing Your DKIM Record

When a new DNS record is created, it can take some time to propagate and be available for querying. Alchemer recommends waiting a few hours following the record being populated before testing. Users may need to wait up to 72 hours for the records to propagate.

an ***MX record*** should be set up prior to attempting to enable DKIM/SPF. Some mail clients may reject emails from domains without an MX Record.

To test for a DKIM record, follow these steps:

1. Via your browser, navigate to <https://mxtoolbox.com/TXTLookup.aspx>.
2. In the **Domain Name** field, enter the domain that you want to test and click the **TXT Lookup** button.
 - To see a successful record, enter `dkimgizmo1._domainkey.alchemer.com` and click **TXT Lookup**. This will show you a return for a correctly configured DKIM record.
 - Next, enter your domain, for example: `surveygizmokey1._domainkey.yourdomain.com` and click **TXT Lookup** to test your domain.



You can also perform an SPF and DKIM check using <https://www.mail-tester.com/spf-dkim-check>.

- To see a successful record, enter `alchemer.com` in the domain name field and `surveygizmokey1._domainkey` in the DKIM Selector field.
- Specifically, with regard to the **DKIM Check**, a successful record will return "Key Length" information. If a key length value cannot be retrieved, you will see, "We were not able to retrieve the key length..." message. Make sure the key was entered correctly and retry.

Additionally, another resource for performing an SPF record check is [DMARC Analyzer](#).

- DMARC enables customers to confirm the SPF record inheritance tree DNS lookup limit of 10 is not exceeded.

Using "Send Test" with Email Campaigns in Alchemer does **NOT** use SMTP/DKIM/SPF settings, and will send from Alchemer's Servers (@surveygizmo.com).

Next Steps

Now that you have configured your SPF & DKIM records, learn about customizing your email **From Address** to use what you have configured:

- [Configure Email Actions to Use DKIM & SPF](#)
- [Configure Email Campaigns to Use DKIM & SPF](#)

FAQs

- ⊕ Why did Alchemer implement SMTP and DKIM/SPF?
- ⊕ Do I need to use SMTP or DKIM/SPF to send email from Alchemer?
- ⊕ Can I set up multiple Custom Email integrations, is there a limit?
- ⊕ What port should I use for SMTP?
- ⊕ Can I use my SMTP or DKIM/SPF integration when emailing Reports or Exports?
- ⊕ Can I use both SMTP and DKIM/SPF Integrations at the same time?
- ⊕ If I want to use multiple/different from addresses, do I need multiple integrations?
- ⊕ How are unsubscribed contacts handled when using a Custom Email Integration?
- ⊕ How can I test and troubleshoot SPF configurations?

Related Articles