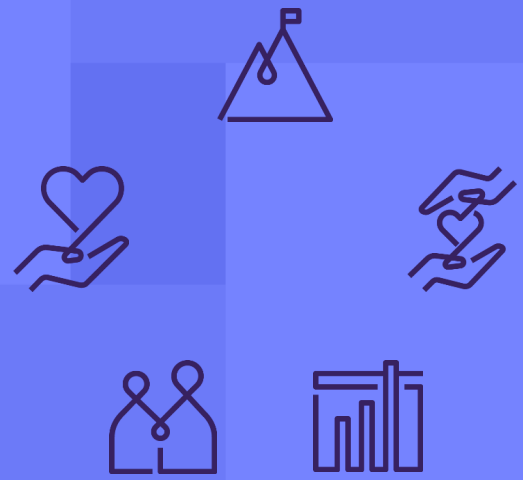
DONOR ENGAGEMENT

Setting Up Your Email



Bonterra™

Meet your Trainer...

Ryan Sauve

Training Specialist

Donor Engagement

EveryAction

Bonterra™

Agenda

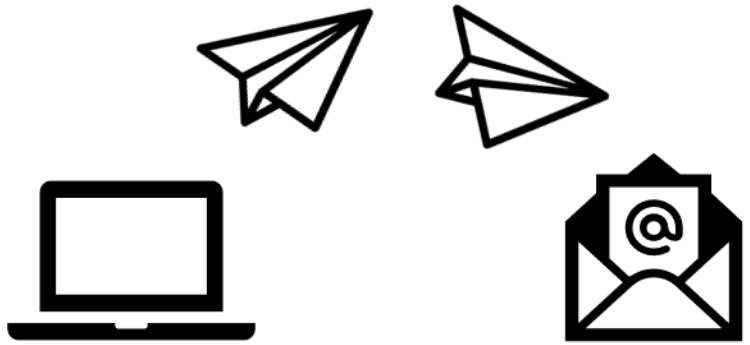
1. Introduction to SPF and DKIM
2. Adding your SPF Record
3. Adding your DKIM Record
4. Validating your SPF Record
5. Validating your DKIM Record
6. DMARC Setup and Why It's Necessary
7. Q&A

Introduction to SPF and DKIM

Bonterra™

What does SPF/DKIM do for emails?

Both **SPF and DKIM** are used in tandem to ensure that your emails are legitimate and not a phishing attempt. Failing to pass an SPF or DKIM check could mean your emails are more likely to end up in the spam/junk folder.

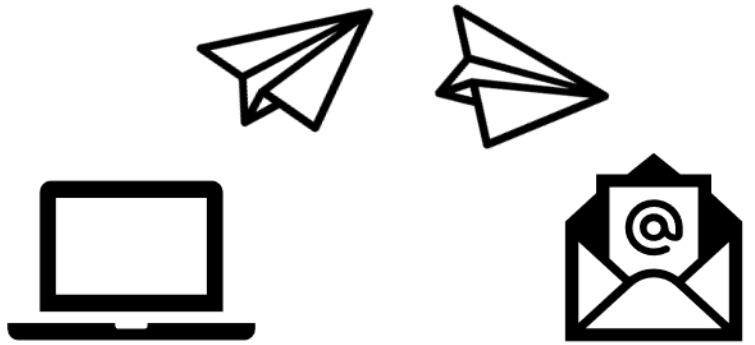


Before We Begin:

- Since **we don't manage the hosting of your organization's domain DNS (**Domain Name System), our support staff are unable to assist you with editing these records.
- If you can't figure out who manages your domain, you can look up your domain at www.whois.net and find the name and email address of the admin for your domain.
- **Please work with your domain administrator** to implement these instructions.

What is SPF?

SPF, or **Sender Policy Framework**, is a generic approval you can add to your domain to approve certain groups to send on your behalf.

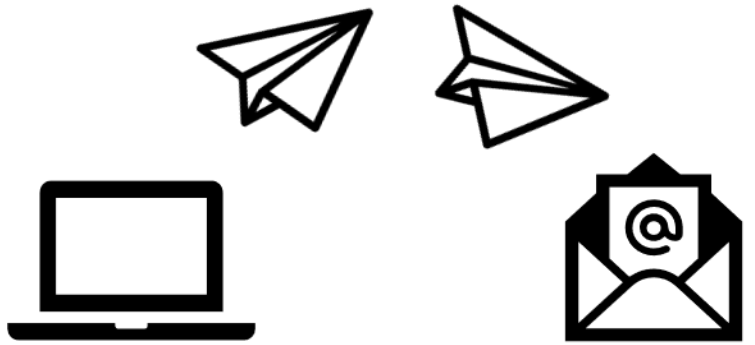


The Basics of SPF:

- Helps receiving servers like Hotmail or Gmail identify fake messages that appear to come from your organization, in addition to making sure your email is sent correctly.
- Includes who you use for your internal email inbox (like GSuite or Office 365) as well as any blast email providers, like us.
- Allow Email Service Providers, like Gmail or Hotmail, to verify that an email from your domain is sent through an IP address you have verified as allowed to send on your behalf.

What is DKIM?

DKIM, or **DomainKeys Identified Mail**, is a digital signature at the top of every email sent that's used to verify the email sent using your domain is an approved message.



The Basics of DKIM:

- It was created for the same reason as SPF to prevent spammers from impersonating you as an email sender. It is simply another was to tell your receivers "Yes this is really me who is sending this message."
- This allows Email Service Providers, like Gmail or Hotmail, to confirm that the DKIM attached by us as we send emails on your behalf match a DKIM record you've added to your domain.

Adding Your SPF Record

Bonterra™

To begin, know that SPF records always begin with V=spf1. This tag defines the record as SPF.

For the SPF TXT record, please modify the existing TXT record that starts with “v=spf1” to add “include:_spfprod.ngpvan.com~all “ after v=spf1.

When finished, it will look like:

v=spf1 include:_spfprod.ngpvan.com~all

You can also modify an already existing SPF record by updating the SPF.

For this example, let's assume you're sending email from G suite by Google. In this case, your SPF record will look like this:

When finished, it will look like:

v=spf1 include:_spf.google.com include:_spfprod.ngpvan.com~all

Here’s another example using Microsoft Outlook.

Let’s say you use the yourorgdomain.org email domain, such as info@yourorg.org, and you also send email from Microsoft 365 and our products only.

When finished, it will look like:

v=spf1 include:spf.protection.outlook.com include:_spfprod.ngpvan.com~all

Generating Your DKIM Record

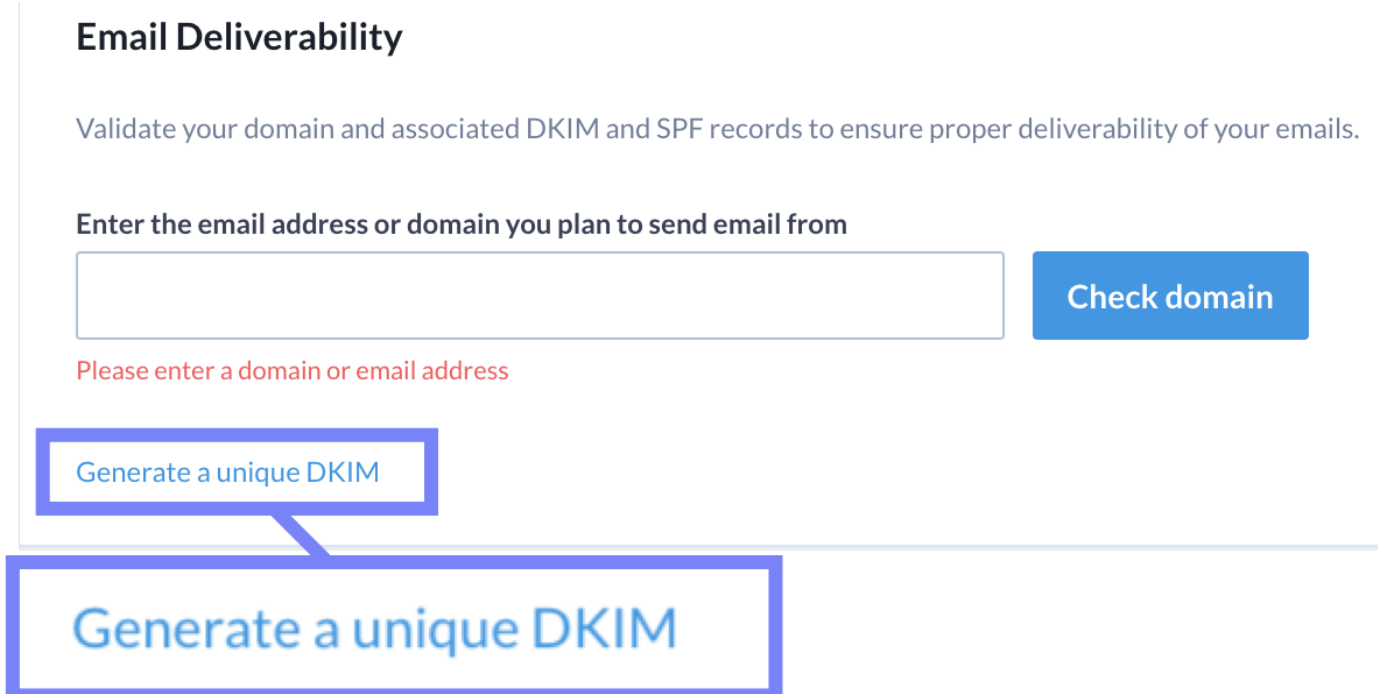
Bonterra™

Safely Generating A DKIM Record

On the same screen as the SPF validation tool, there is also a clickable link available to generate your own DKIM key.

As all DKIM keys will be unique, per sending domain, this process may need to be repeated if you're sending from multiple *separate* domains.

Once the **Generate a unique DKIM** button is clicked, you will then be prompted to enter your domain, which then generates your key.

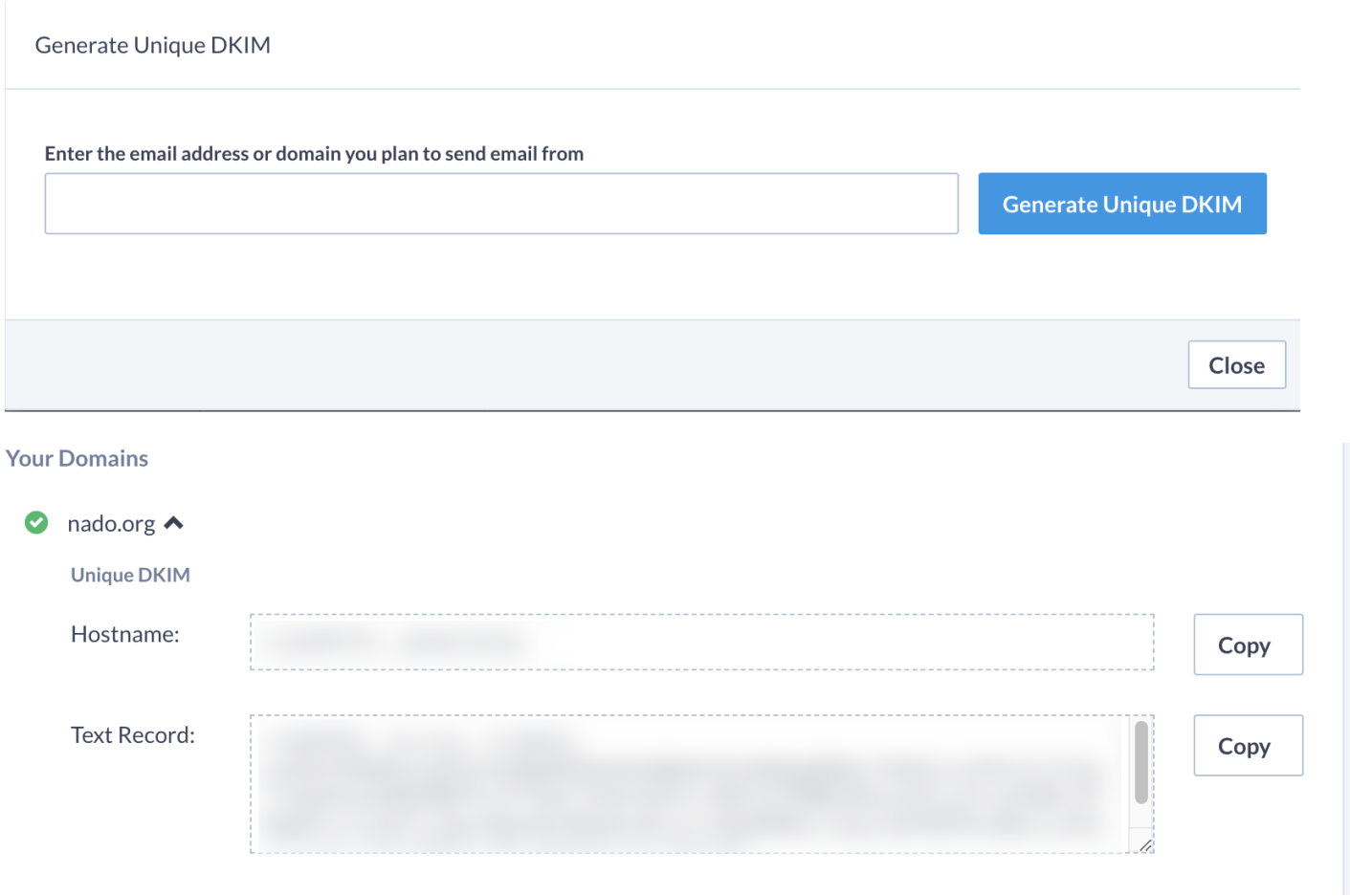


Safely Generating A DKIM Record (cont'd)

First, enter your sending domain. Then, click **Generate Unique DKIM.**

Once clicked, you'll be presented with a unique Hostname and Text Record that are copyable for submission to either your IT department, domain hosts, or responsible staffperson.

It is highly recommended that you leverage these Copy buttons to avoid any unintentional cuts or added characters within these keys, as they **must** be used as provided.

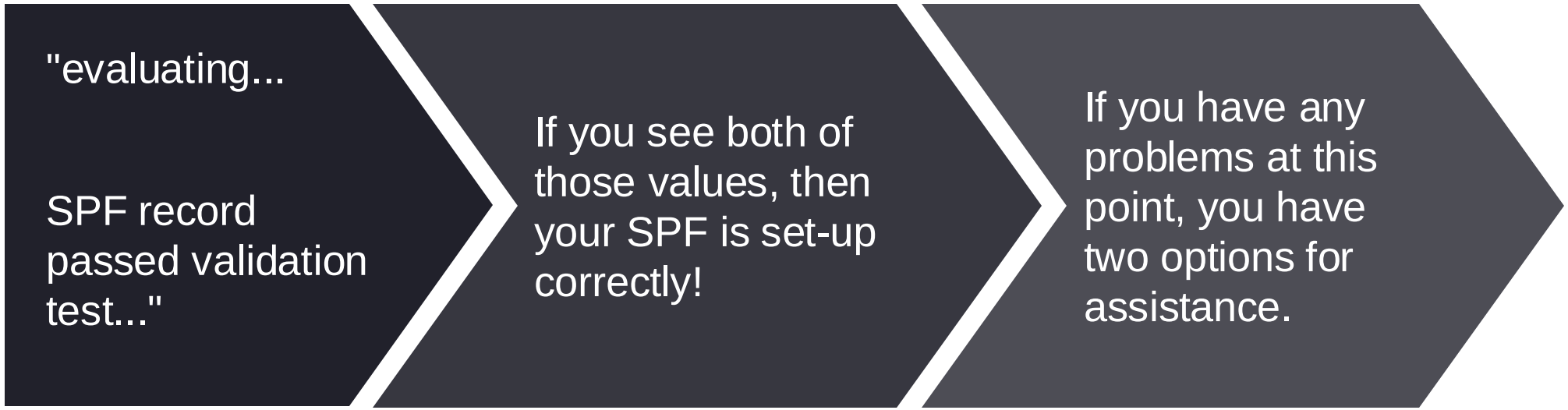


Validating Your SPF Record

Bonterra™

To test your SPF record, please click this link: https://www.kitterman.com/spf/validate.html

After entering your sending domain (yourorganization domain.org) into the first field, you should see "include:_spfprod.EveryActionvan.com" in the spf return value with a resulting value of:



1. Help Center Article Support:

   How to: Configure my DKIM or SPF for email Deliverability

2. Reaching out to your DNS provider, or whoever manages your domain

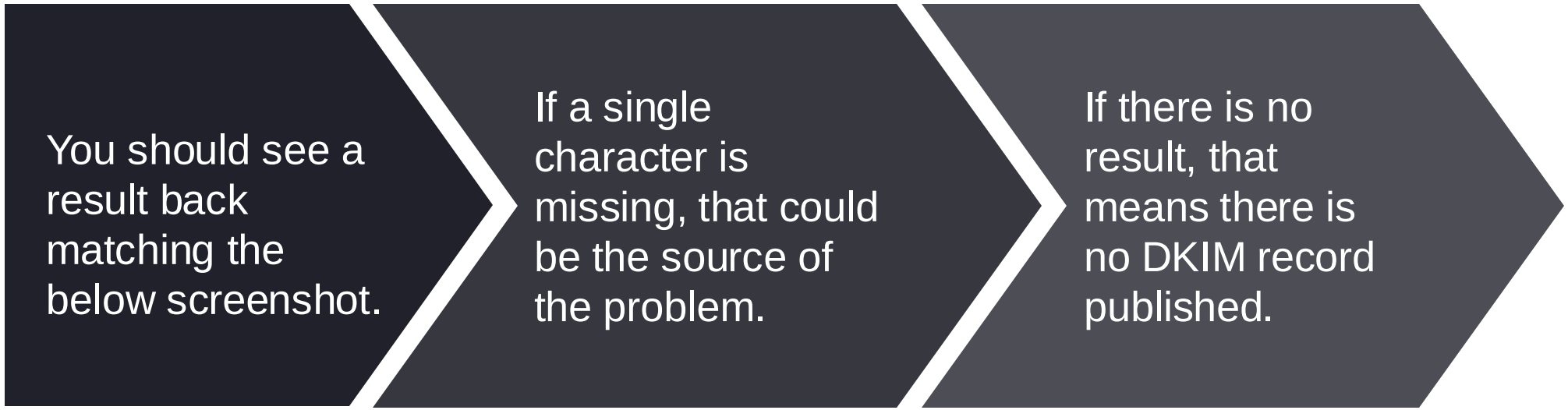
Bonterra

Validating Your DKIM Record

Bonterra™

To test your DKIM record, please click this link: https://mxtoolbox.com/dkim.aspx

Enter your domain (yourorganizationdomain.org)



1. Help Center Article Support:

   How to: Configure my DKIM or SPF for email Deliverability

2. Reaching out to your DNS provider, or whoever manages your domain

DMARC Setup and Why It's Necessary

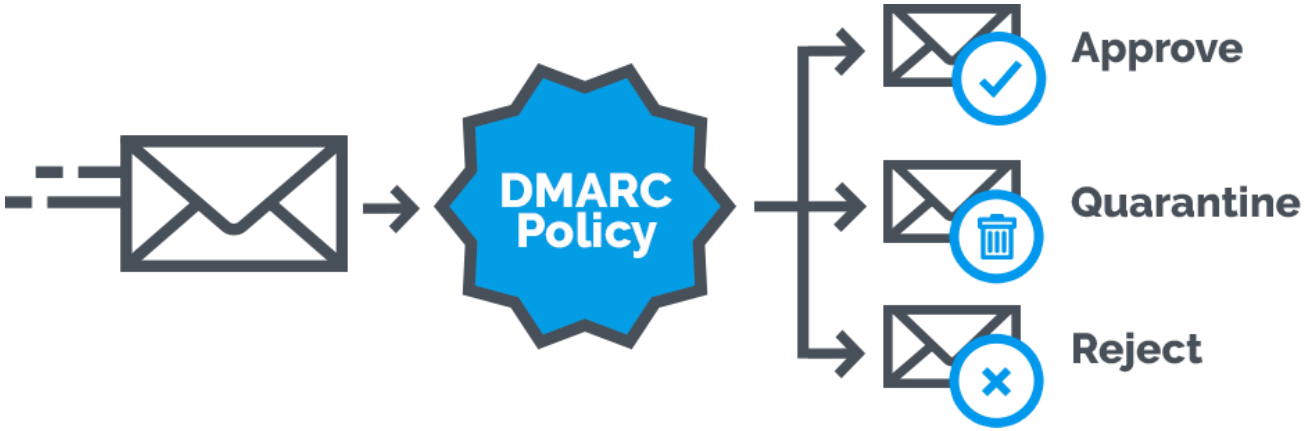
Bonterra™

What is DMARC?

DMARC: Domain-Based Message Authentication, Reporting and Conformance

This is an add-on to email authentication that prevents bad actors from spoofing or impersonating your domain in their sends.

- DMARC has three policy settings (None, Quarantine, and Reject)
- Yahoo and Google require at least “None” today, but we think they will require quarantine or reject in the future.
- For a full explanation of DMARC in-depth, please check out https://dmarc.org/



To Ensure Smooth Deliverability

Google and Yahoo announced new sender requirements back in October 2023.

- Authenticate mail with DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF).
- Implement DMARC domain security.
  - Implement easy unsubscribe (and one click unsubscribe via special header).
  - Keep complaint rates low.
- Learn more directly from Google about these changes.

Creating Your DMARC Record

As this process is similar to the setup of DKIM and SPF, we have a full guide available here for all end users.

For an overview, the process requires:

1. Gaining access to the service that hosts your domain's DNS record (Cloudflare, Godaddy, etc.).

2. Checking that both SPF and DKIM records have been created for your domain. You can use the SPF and DKIM checker in Targeted Email's Deliverability settings page.

3. Once you've verified that your DKIM record exists, add a new TXT record in your DNS host which will hold your DMARC information. This record should be added to your apex domain (your domain without any subdomains, for example, mydomain.com, not subdomain.mydomain.com). A basic DMARC record would look like this:

_dmarc.mydomain.com TXT v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.org

NOTE: rua= is an optional parameter. Mailbox providers will regularly email reports of your domain's usage on their platform. This can be helpful but also generate a lot of email. You can use an email address from your organization but we suggest using a DMARC monitoring service and inserting their provided email address.

4. Once your DMARC record is created, check that it is aligned correctly with your DKIM record.

Q&A

Bonterra™

Additional Resources

Bonterra™

Support

- Contact your System Administrator
- Email help@EveryAction.com
- Call (202) 370-8050
- Submit a Support Request Ticket from the Main Menu of the EveryAction CRM

Bonterra™

Help Center Resources

- How to: Configure my DKIM or SPF for Email Deliverability
- Tutorial: Configuring SPF/DKIM for Email Deliverability
- Troubleshooting: SPF/DKIM Setups
- Configuring DMARC to work with Targeted Email

Additional Training

- Bonterra Academy: https://help.everyaction.com/s/article/Bonterra-Academy-Self-Signup
  - Foundational Webinar Series
  - Upcoming initiatives
  - Videos in Bonterra Academy

Feedback & Training Survey

- Please fill out our 1-minute survey that appears after the webinar.
- Access the survey here: Training Feedback Survey

Bonterra™

Thank You for Attending!

Bonterra™