SUMMARY

Ethnio uses three industry-standard providers, Mailgun, Sendgrid, and Amazon SES, to send emails with maximum deliverability using any email from/sender/reply-to addresses our customers prefer. Ethnio frequently has to email your respondents and participants, to save you time, for things like automatic scheduling or incentive payments. Each of our providers has different uses and varying levels of deliverability, but our average deliverability is around 88%. This depends largely on which of the three levels you choose for your Ethnio account, and keep in mind that Level 2 and above is only available for Enterprise accounts.

IN THIS DOCUMENT - DOMAIN VERIFICATION OPTIONS

LEVEL 1 — By default, Ethnio sends email using the header “on behalf of”

LEVEL 2 — DKIM / SPF

LEVEL 3 — SMTP Authorization for a single address
LEVEL 1: “ON BEHALF OF”

The default method of sending emails to your participants in Ethnio requires no integration or domain verification from your organization. **Out of the box, it offers about 85% deliverability.** Let’s say your email is research@acme.com and you want to use Ethnio for Scheduling and incentive payments, as part of your job as Research Coordinator at Acme Corporation.

You would simply login to your Ethnio account, enter **Acme Research / research@acme.com**, and when your respondents reply to the email it will go to you. A small percentage of users (2-12%) will see “Ethnio on behalf of Acme Research” as the from address, but the reply-to will always be research@acme.com.
This means that when any of your participants respond to an Ethnio-generated email, the email will always go back to you, and not Ethnio.

**ISSUES WITH LEVEL 1**

Some percentage of your participants will never get the email, because it will go to spam, and some participants will see “Ethnio on behalf of Acme Research,” and not trust that it’s from you, since phishing is always a concern. If you have a lot of research volume, or use keywords in your email that trigger spam reports, this can also damage the email reputation of both Ethnio and your organization. This is extremely rare, but it’s part of the world of automated email distribution that every company deals with. If you’d like to ensure higher deliverability and the minimum lost emails due to spam or trust, see the next two levels.
LEVEL 2: DKIM/SPF

If you’d like to increase deliverability over Level 1, ensure nobody ever sees the Ethnio domain, make sure no unnecessary spam reporting happens, and prevent any phishing concerns, you can configure your domain for allowing Ethnio to send emails through either Mailgun or Sendgrid. This is a custom add-on as part of an Enterprise package, and has to be verified by setting up the SPF and DKIM records to your domain provider’s DNS management section.

The DKIM or Domain Keys Identified Mail is an encryption authentication method that is used to ensure that the email is originated from an authorized system and it prevents spammers from stealing the identity of legitimate entities. Whereas SPF or Sender Policy Framework is used to improve email reliability and prevent spoofing.
The SPF and DKIM DNS records allow Ethnio, using either Mailgun or Sendgrid, to deliver email for our customers and any email address at their domain. So that could be uxresearch@acme.com or bob@acme.com or lisa@acme.com. There are no restrictions on how many different emails can be used inside Ethnio with this level. See below for an example of the domain verification dashboard we’ll setup for you in Ethnio to get everything setup, and track authentication.

ISSUES WITH LEVEL 2

Each domain, development environment, set of DNS rules, and organization is different. There can be restrictions at your organization for SPF/DKIM and which vendors are allowed to go through this process. You could already be using Sendgrid or Mailgun directly, which would block Ethnio. It usually requires a heavy security and technical audit of Ethnio, and our pricing for this integration add-on has to reflect that process.
LEVEL 3: SMTP AUTHORIZATION

If your organization doesn’t want to approve the DKIM/SPF framework for Ethnio, the last option is to authorize Ethnio to send from one single email address using a couple different options for SMTP authorization. This means, for our example, that only research@acme.com would work inside Ethnio, and no other addresses. Each tool we use for email distribution has unique requirements for SMTP relays or authorization and sending mass emails, so this level requires the most custom work on Ethnio’s side.

QUESTIONS, CUSTOM EMAIL FEATURES, CONCERNS ETC...

Any questions? Happy to help with any additional reports or audits. Please email info@ethn.io or call us at (888) 879 7439 for more information.