

BI Helper Secure Email

Set up a branded sending domain

Updated: May 10, 2024

AWS SES and Email Structure	2
BI Helper Send Email tab	2
Recipient Inbox	2
Set Up a Branded Sending Domain	3
DMARC Compliance	3
Setup Steps	3
Choosing 'Mail From' Domain	3
Aligning 'From' Address with 'Mail From' Domain	4
Additional Resources	4

AWS SES and Email Structure

BI Helper uses [AWS SES](#) (Amazon Simple Email Service) to send emails. Emails delivered via BI Helper - AWS SES have two components:

1. From email (the address you specify in the BI Helper email setup screen).
2. 'Mail from' domain (the domain via which the emails are delivered. The default domain is [amazonses.com](#))

BI Helper Send Email tab

Send emails ⓘ



From email ⓘ

BI Helper Demo <demo@bihelper.tech>

Verify this email

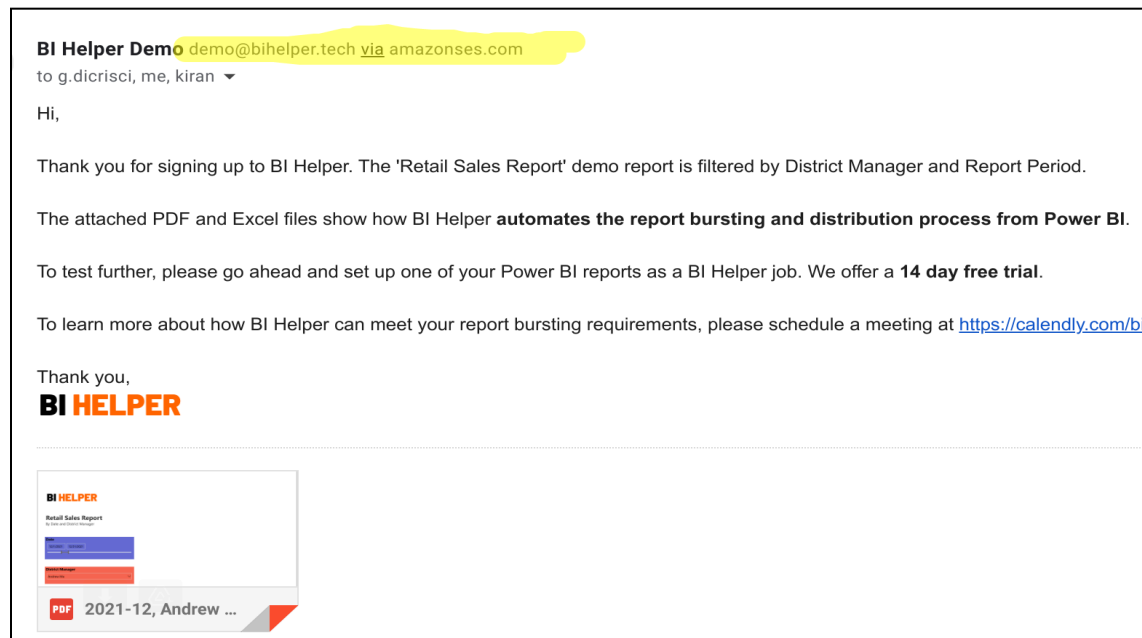
Email subject

Test PDF : \${File Name }

Eg: Test PDF: 2019-04, Allan Guinot

Recipient Inbox

This is how the email appears in the recipient's inbox. Note that amazonses.com is the 'mail from' domain.



Set Up a Branded Sending Domain

Branded sending domains also known as dedicated sending domains or 'mail from' domains:

- Give you better deliverability. Email servers can flag the emails coming from BI Helper since there is a domain mismatch between the 'from' address and the 'mail from' domain.
- They also improve your branding in the 'from' address in the inbox by removing the 'sent via amazonses.com' disclaimer.
- Make your emails [DMARC compliant](#).

DMARC Compliance

By using a branded sending domain, you have the flexibility to use SPF, DKIM, or both to achieve Domain-based Message Authentication, Reporting, and Conformance (DMARC) validation. DMARC enables a sender's domain to indicate that emails sent from the domain are protected by one or more authentication systems.

Setup Steps

To set up a branded sending domain, the following steps need to be followed:

1. The user needs to share their 'mail from' subdomain with support@bihelper.tech, the requirements for which are [listed here](#).
2. BI Helper Support will then share the TXT, MX and CNAME records for SPF and DKIM with the user, who has to publish them to their DNS provider.
3. Detection of these records can take up to 72 hours. The user will be notified by their DNS provider once their domain has been verified.
4. The user finally needs to align their 'From' address with their 'mail from' domain, as detailed [here](#).

Choosing 'Mail From' Domain

The subdomain used for the 'mail from' domain has to meet the following requirements:

-
1. The 'mail from' domain has to be a subdomain of the primary domain that users send their email from. For example, 'reports.example.com' is a valid 'mail from' domain for the domain 'example.com'.
 2. The 'mail from' domain should NOT be the domain that users send their email from.
 3. The 'mail from' domain should NOT be a domain used to receive email.

Aligning 'From' Address with 'Mail From' Domain

To be DMARC compliant, the domain in the 'from' address must align with the root domain in the 'mail from' sending domain.

So if the 'mail from' domain is reports.example.com, the root domain is example.com. Therefore, using hello@example.com as the 'from' address is in alignment with the root domain.

Additional Resources

More details about the 'mail from' domain, DMARC compliance, and AWS SES are at

<https://docs.aws.amazon.com/ses/latest/dg/mail-from.html>

- **End of document**