BI HELPER

Email Authentication in BI Helper

Set up a branded sending domain for secure email delivery

Updated: September 3, 2025

Why Email Authentication is Important

Email is one of the most prominent channels for cyberattacks in organizations because it is the most popular method for corporate communication. Unauthenticated domains are highly vulnerable to phishing and other malicious activities. According to research by Verizon in 2024, 90% of all malware is delivered by email, making it critical for organizations to differentiate between real and fake emails.

Email authentication is an effective process to confirm the identity of email senders. It plays a critical role in any email-based business by helping users distinguish legitimate emails from spam and phishing emails to limit the risk of cyberattacks.

The foundational protocols in email authentication that **collectively enhance trust** and **email deliverability** are:

- Domain-based Message Authentication, Reporting and Conformance (**DMARC**) - Helps domain owners ensure that emails are sent from their domains, and control how they want unauthorized messages to be treated.
- Sender Policy Framework (**SPF**) - Authenticates emails by helping organizations publish an authorized list of senders.
- DomainKeys Identified Mail (**DKIM**) - Uses digital signatures to sign emails and ensure that they remain unaltered through the delivery process.

For organizations sending more than 5,000 emails daily, **DMARC compliance** is a **requirement** for inbox placement with leading email providers like Gmail, Yahoo and Outlook. DMARC validation ensures that:

- Emails are genuinely sent from the user's domain using SPF and/or DKIM checks.
- Spoofing and phishing are prevented by giving inbox providers clear instructions on how to handle unauthenticated messages.
- Reporting is enabled so that domain owners can monitor authentication results and spot any abuse.

For smaller volume email senders, these leading email providers have started **flagging DMARC non-compliant emails**. Instead of being delivered to the recipient's Inbox, non-compliant mails often end up in the Junk/Spam folder, in the Other tab (in Outlook) or get archived or redirected by rules set up by the user.

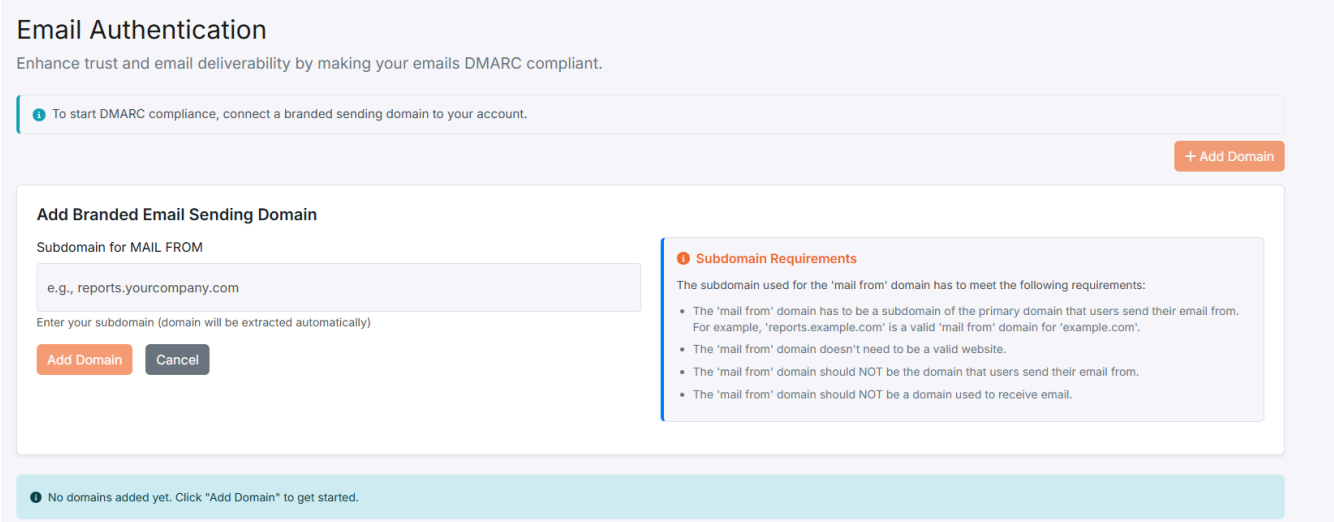
DMARC Compliance in BI Helper

Branded Email Sending Subdomain

In order to be DMARC compliant, you need to connect a branded email sending subdomain to your account that matches the root domain in your 'from' email address. For example, if your root domain is *mycompany.com* and you send emails from sales@mycompany.com, then *reports.mycompany.com* can be a branded email sending subdomain.

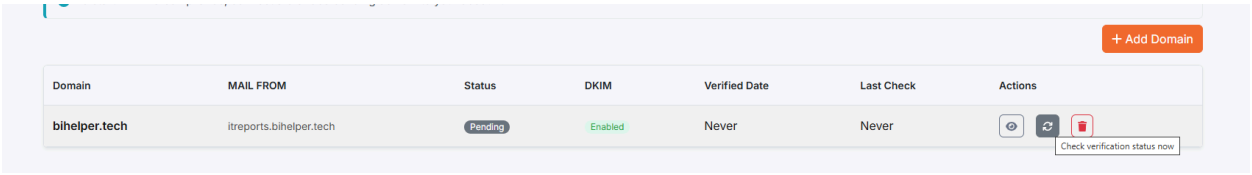
Setup Steps

- Go to Settings > Email Authentication in BI Helper and click on the '+Add Subdomain' button.



- Enter your chosen subdomain and click on 'Save'. BI Helper will generate 3 CNAME records, 2 TXT records and one MX record for SPF and DKIM in the same page. Please copy and publish them to your DNS provider. Click on 'Continue' to complete the DMARC setup.

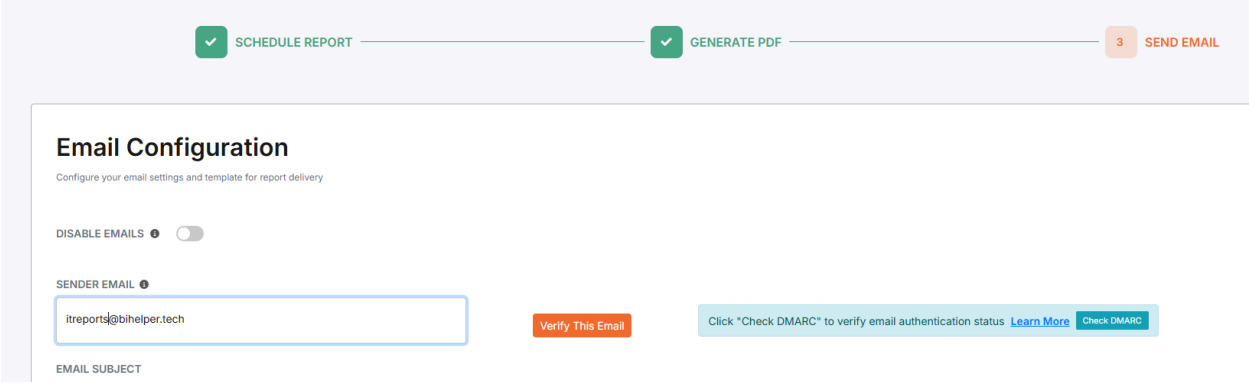
- Allow up to 72 hours for your DNS provider to propagate them. You can check the DMARC status in the below table in the same page.



- Once your domain is verified, please ensure that your ‘from’ address is aligned with your ‘mail from’ subdomain.

Check DMARC Status of ‘From’ Email

To check the DMARC status of your ‘From’ email ID, go to the Job Summary page and click on the Edit Job icon. Then go to the Send Email tab, enter your Sender Email ID and click on Check DMARC.



Additional Resources

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

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

- **End of document**