Email Authentication for DMARC, SPF, and DKIM

Last Modified on 12/05/2023 7:47 am CST

> **Infinite Campus does not have access to individual customer email configurations and cannot directly assist with configuring SPF/DKIM/DMARC.**
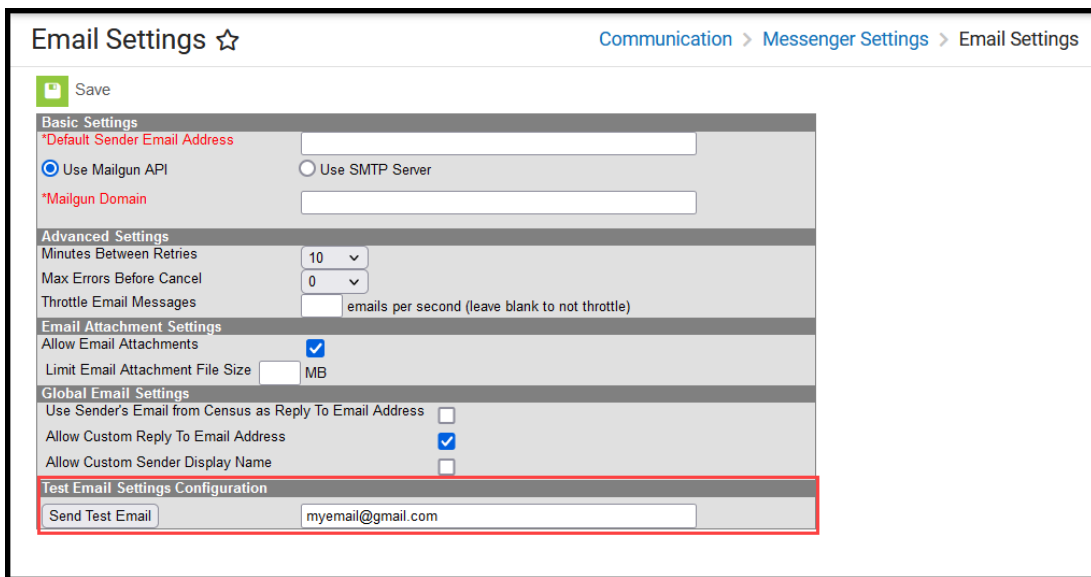
Does This Affect You? | What Are Google's and Yahoo's New Requirements? | What do I need to do? | Need Assistance?

Google and Yahoo now require enhanced email authentication, specifically through DMARC, SPF, and DKIM starting **February 1st, 2024**. To ensure uninterrupted email delivery to Google/Gmail and Yahoo recipients (e.g., @gmail.com, @yahoo.com, or any district-created email accounts via admin.google.com), your district's DNS (Domain Name System) records must be accurately configured. Campus Support will be creating a Support case for districts using Campus Mailgun Relay that need to have Mailgun settings updated to meet the Gmail and Yahoo requirements.

Does This Affect You?

To check if your district is affected:

1. In Infinite Campus, navigate to Email Settings.
2. Send a test email to a Gmail address. (If you do not receive any test email at that Gmail account, your email configurations need to be reviewed with the email relay provider, as they may be incorrect.)
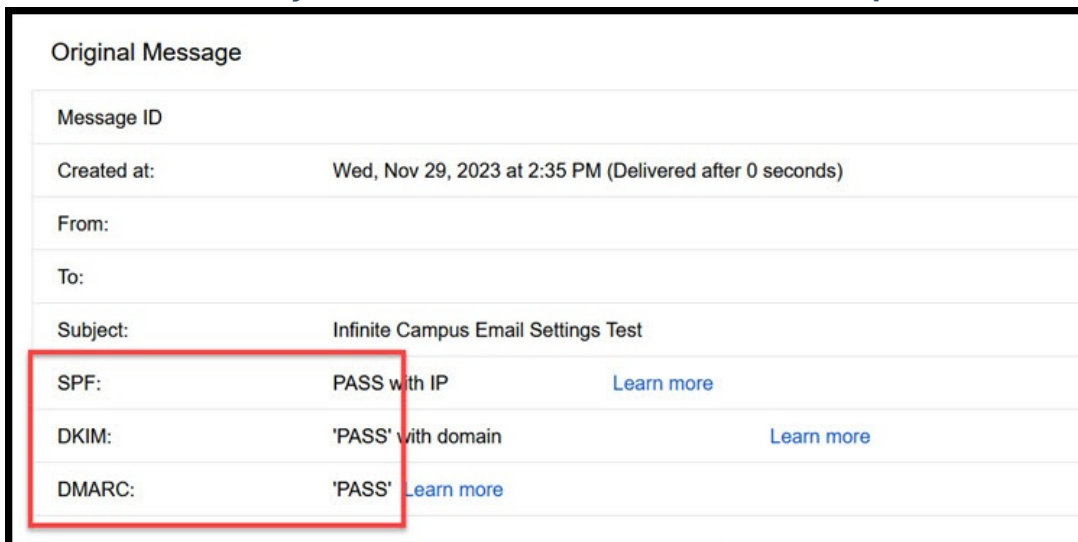

3. In your Gmail account, select the received email, click the ellipsis to the right of the email - ⋮ and select **Show original.**
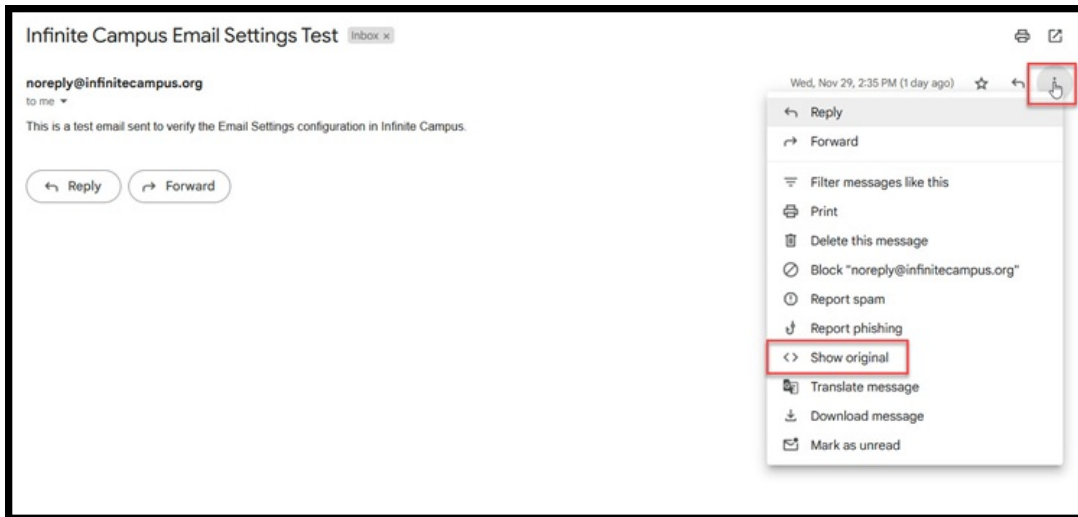
4. In the **Original Message**, look for PASS under SPF, DKIM, and DMARC. **If PASS is not visible for all three, your district is affected and action is required.**

If your sending domain does not have SFP, DKIM, and DMARC configured, this may prevent your emails from reaching Google/Gmail and Yahoo recipients after February 1st.

What Are Google's and Yahoo's New Requirements?

The requirements include configuring SPF, DKIM, and DMARC. These are security protocols that help protect against email spoofing and phishing attempts by ensuring that email messages are sent from legitimate sources.

- **SPF** is a way to specify which mail servers your domain uses to send mail, helping mail

servers ensure the email is genuinely from your domain.
- **DKIM** is a way to add a digital signature to emails which mail servers can use to confirm your domain sent the email.
- **DMARC** is a way to establish a policy that tells mail servers what to do with emails that do not pass SPF or DKIM checks.

Infinite Campus has taken steps to ensure DMARC is implemented for outgoing emails from our end. Now, each customer must verify and enable SPF, DKIM, and DMARC for their individual email sending domains.

What do I need to do?

This involves changes to your email sending domain's DNS records and must be managed on your end by your district's IT team or domain owner.

1. **Have your district's domain owner configure SPF, DKIM, and DMARC.**
2. **Monitor reports:** Regularly review DMARC reports to identify and address potential issues. Various monitoring services exist, including a free monitoring weekly email digest.

> **Infinite Campus does not have access to individual customer email configurations and cannot directly assist with configuring SPF/DKIM/DMARC.**

Need Assistance?

If you are unsure about the status of DMARC for your domain or need guidance on how to set it up, we recommend reaching out to your IT department or email hosting provider. They have the expertise to assist you with the necessary configurations. You may also find these support tools and communities helpful:

- Tools like dmarcguide.globalcyberalliance.org can help give guidance on the process of configuring DMARC, SPF, and DKIM.
- StackExchange Webmasters Forum
- Reddit's DMARC subreddit
- Global Cyber Alliance Forms