

Configuring Gmail with Less Secure App Access

Configuring GMail email feature in HS4 with less secure apps.

The HS4 software is capable of sending emails when triggers are activated or even scanning emails for keywords to then activate your events. We recommend using a Gmail account as HS4 has the advanced settings ready for Gmail, but you can use a different email provider if you prefer and know the SMTP settings for it. If you are unsure of those settings, use Gmail.


The security settings outlined below must be adjusted as described for Gmail to work. Due to these security concessions, **we recommend creating a new, dummy Gmail account exclusively for use with HS3.**

Allow Less Secure Apps


1. Visit mail.google.com, then log into your Gmail account.
2. After logging in, you will see your profile picture or icon in the top right corner. Click on that, then blue **Google Account** button.
3. From here, click the **Security** section on the left-hand side of the screen.
4. Scroll to the bottom of the page, and you will see the **Less Secure App Access** section. Click the **Turn on access** button.

Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account. To keep your account secure, Google will automatically turn this setting OFF if it's not being used. [Learn more](#)

 On

[Turn off access \(recommended\)](#)



About Multi-factor Authentication

It is generally a good idea to enable multi-factor authentication on any online account to prevent unwanted logins. However, having such a security feature enabled on your Gmail account will prevent your HS3 system from being able to access your account, unfortunately.