GMail for emails with MBS Plugin

As you may know we have support for sending and receiving emails with our MBS FileMaker Plugin and MBS Xojo Plugins. Using CURL functions we do the transfers for SMTP, POP3 and IMAP. Our SendMail functions help assemble emails including html content, inline graphics and multiple attachments. All with proper text encoding, so your umlauts or asian characters survive. The EmailParser functions help to parse emails and our IMAP Email example shows how to use them to load emails and preview them in a web viewer.

Now Gmail has some security enhancements. And you can use a few ways. In general if you use an account for automating processing of emails, it may be good to make a separate account. Don't use your main account, but maybe have an extra gmail account to send your emails and process the bounces. Keep this separate to your other accounts.

1. Access by less secure applications

Gmail has an option to allow use of less secure applications.
You can enable that option and then just use your login to gmail for our email functionality.
Here are some sample script lines:
\# set server without SSL here, as we enable TLS later
Set Variable [$r ; Value: MBS("SendMail.SetSMTPServer"; $EmailID; "smtp.gmail.com")]
\# put in your login here
Set Variable [$r ; Value: MBS("SendMail.SetSMTPUserName"; $EmailID; "monkeybreadsoftware@gmail.com")]
Set Variable [$r ; Value: MBS("SendMail.SetSMTPPassword"; $EmailID; "MonkeyLikesToSendEmail")]

And later in the script configure CURL:
\# This turns TLS on and requires connection to be encrypted
Set Variable [$r ; Value: MBS("CURL.SetOptionUseSSL"; $curl; 3)]
\# force TLS version 1.2 or newer
Set Variable [$r ; Value: MBS("CURL.SetOptionSSLVersion"; $curl; 6)]
\# You may want to put in the root certificate related for google. We have the cacert-google.pem file on our blog, which contains the GlobalSign Root CA - R2 used by Google. By using only this certificate, you can avoid a man in the middle attack with a gmail.com certificate from another CA. Since the cacert expires someday, you may need to

update that every few years.
Set Variable [$r ; Value: MBS("CURL.SetOptionCAINFO"; $curl; "/
Users/cs/Documents/cacert-google.pem")]
now enable full verification:
Set Variable [$r ; Value: MBS("CURL.SetOptionSSLVerifyHost"; $curl;
2)]
Set Variable [$r ; Value: MBS("CURL.SetOptionSSLVerifyPeer"; $curl;
1)]

This seems to work as of April 2021. But better use the following
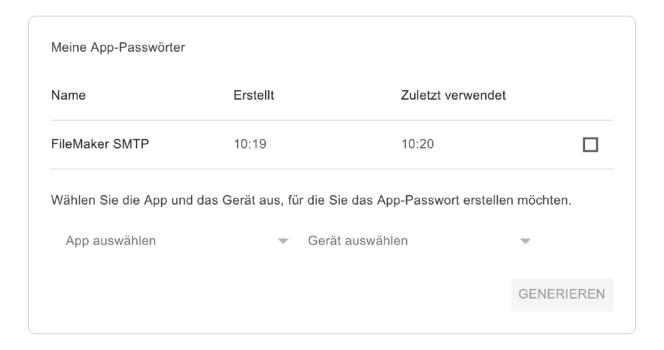method:

2. App Passwords

Now you should have a 2 factor authentication enabled for your
account. And once you have it, always be cautious if you see a request
coming to your device. Whenever you login, you will be asked for a
token, which comes via sms or app. Eventually someday there may be
a hacker, who got your right password and tries to login. Then please
don't grant access and don't tell anyone the code you get. Not that
someone is on the phone and tells you to read the code google sends to
you to enter a lottery.

Once 2 factor authentication is enabled, the security settings website
from Google shows App-Password section. There you can create a new
one by selecting app and then device. I select Email in left and other
use in right popup. Then it shows a text field and I just enter "FileMaker
SMTP" and generate button. A new password like oagveoxdhvgzxnhr is
created. We copy this password in our example and we can send
emails. Once you send an email, the app password website shows the
last usage time:

☐ **App-Passwörter**

Mithilfe von App-Passwörtern können Sie sich auf Geräten, die die Bestätigung in zwei Schritten nicht unterstützen, über Apps in Ihrem Google-Konto anmelden. Sie müssen das Passwort nur einmal eingeben und es sich daher nicht merken. Weitere Informationen

Meine App-Passwörter

Name	Erstellt	Zuletzt verwendet	
FileMaker SMTP	10:19	10:20	☐

Wählen Sie die App und das Gerät aus, für die Sie das App-Passwort erstellen möchten.

App auswählen   ▼   Gerät auswählen   ▼

GENERIEREN

Screenshot is in German, so your texts may be in a different language. The script to send emails with look same as above, just with a different password.

3. oAuth

You can also use oAuth to authenticate. Perform the login and get the bearer token, then pass it to CURL.SetOptionXOAuth2Bearer to do the login via CURL.

Since MBS FileMaker Plugin an do various login options, you may want to use CURL.SetOptionLoginOptions to set which one to use. We can do PLAIN, LOGIN, XOAUTH2, XOAUTH or GSSAPI.
e.g.
Set Variable [$r ; Value: MBS("CURL.SetOptionLoginOptions"; $curl; "AUTH=LOGIN")]

Let us know if you have questions. Please use 2 Factor authentication and be careful on when you grant access.