

Scan Error - 2 Factor Authentication

Technical Services would like to inform you that as of May 30th, Gmail will no longer allow the Less secure app option and it will no longer be available as a selection. In the past, Lexmark devices required this option to successfully send mail.

Going forward, to successfully scan to email using your Gmail account, it is now required to use App/Device passwords after enabling 2 factor authentication. The instructions on the following pages will outline the steps necessary to continue to use this function, bypassing 2 factor authentication.

Less secure app access

To protect your account, apps and devices that use less secure sign-in technology are blocked. To keep your account secure, Google will automatically turn this setting OFF if it's not being used.



On May 30, 2022, this setting will no longer be available. [Learn more](#)

Off



On May 30, you may lose access to apps that are using less secure sign-in technology

 [syzovsk@123@gmail.com](#)

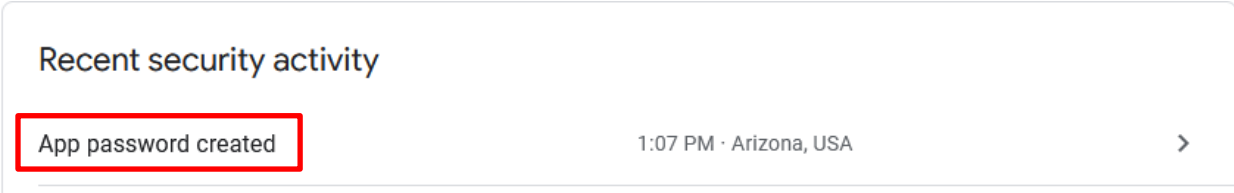
To help keep your account secure, Google will no longer support the use of third-party apps or devices which ask you to sign in to your Google Account using only your username and password. Instead, you'll need to sign in using [Sign in with Google](#) or other more secure technologies, like OAuth 2.0. [Learn more](#)

What do you need to do?

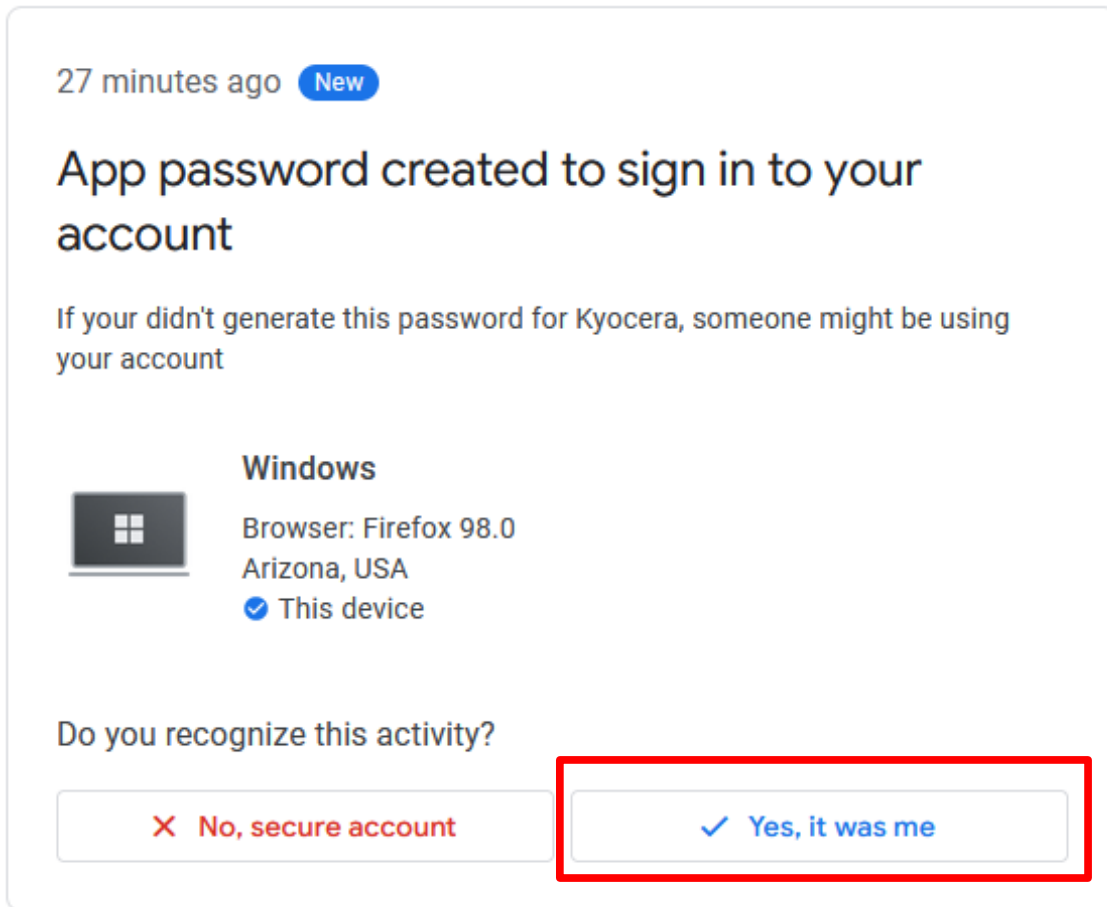
Email software, like Outlook 2016 or earlier, has less secure access to your Gmail. Switch to Office 365, Outlook 2019 or newer, or any other email software where you can sign in using **Sign in with Google**.

[Learn more](#)

8. Go back to your google account under Security and select "Recent security activity". Select the recent entry for App password.



9. Select "Yes, it was me" to confirm change



10. Go to your Lexmark Device's web interface by typing the device's IP into a web browser. If you need help finding the IP please follow the instructions below:

- a. Go to your Lexmark device
- b. Locate the IP address listed at the very top of the screen

9. Select Settings from the left hand side and enter in this information for each field:

- a. Primary SMTP Gateway: smtp.gmail.com
- b. Primary SMTP Gateway port: 587
- c. Reply Address: DoNotReply.getaos@gmail.com
- d. Use SSL/TLS: Negotiate
- e. SMTP Server Authentication: Login/Plain
- f. Device Initiated e-Mail: Use Device SMTP Credentials
- g. User Initiated e-Mail: Use Device SMTP Credentials
- h. Device User ID: DoNotReply.getaos@gmail.com

10. When you get to device password paste in your copied password from step 7

Select Option

- Status
- Settings
- Device
- Print
- Paper
- Copy
- Fax
- E-mail
- FTP
- USB Drive
- Network/Ports
- Security
- Cloud Services
- Reports
- Address Book
- Shortcuts
- Bookmarks
- Apps
- Site Map

E-mail

E-mail Setup

Primary SMTP Gateway Required.

Primary SMTP Gateway Port Range: 1-65535. Default = 25.

Secondary SMTP Gateway

Secondary SMTP Gateway Port Range: 1-65535. Default = 25.

SMTP Timeout Range: 5-30 seconds

Reply Address

Always use SMTP default Reply Address

Use SSL/TLS

Require Trusted Certificate

SMTP Server Authentication

Device-Initiated E-mail E-Mail Alerts, Fax Forwarding, etc.

User-Initiated E-mail

Use Active Directory Device Credentials

Device Userid

Device Password *Required for some Authentication Types.*

Kerberos 5 REALM

NTLM Domain *Required for NTLM Authentication.*

Disable "SMTP server not set up" error

dzcs bggw kgid qtdo

11. Select "save" at the bottom of the page.