Microsoft O365 Modern Authentication/OAuth 2.0 Authentication
Copier Setup Only (Email account setup is a separate process)

Ricoh has been made aware of Microsoft's decision to discontinue support for basic authentication for sending emails using the SMTP protocol in Exchange Online as of April 2026. Following this change, OAuth2.0 authentication will be required on applications and devices when using the SMTP protocol to send emails.

Pre-Requisites & Permissions needed

- Your Ricoh Multi-Function Device must be running Firmware that supports OAuth 2.0 Authentication
- IP Address/Hostname of Ricoh Multi-Function Device
- Admin Access to the Multi-Function Device Web Image Monitor
- Admin Access to O365 Tenant
    - Used to create and license an O365 account for scans to be sent from
        - In the event that a new account is not created as a part of this process, Admin will need to Allow an App request as part of the setup process
        - Email account setting being used must have Authenticated SMTP set (see Troubleshooting below for details)
- Port 587 must be opened on the Firewall

A) Firmware (Ricoh device will require a firmware update to support OAuth 2.0)

To configure Ricoh MFP, Firmware needs to be updated before beginning configuration changes. Contact our Service Department for instructions on updating device firmware.

Firmware Sources:

- Ricoh Firmware Update Tool on the Ricoh Site (Customer access)
    - Download the universal update tool: RICOH Firmware Update Tool Downloads | Ricoh Global
    - Run this and follow the instructions to add the device and update firmware.

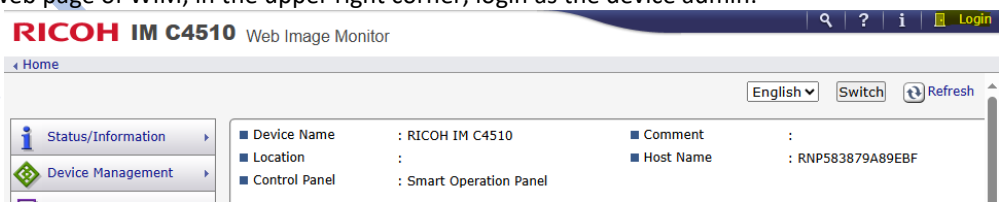
B) Configure for OAuth 2.0

To access the configuration SMTP settings you will need to use Web Image Monitor (WIM) by entering the device IP address into your web browser address bar: Enter “http://(IP address of the machine)/” and then press Enter.

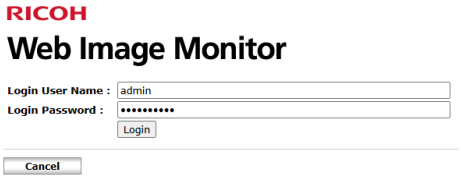
*Note: This cannot be configured at the copier control panel.

*Note: Click here to find your device IP address: How-to-Find-the-IP-Address-of-Your-Ricoh-Copier.pdf

1) On the web page of WIM, in the upper right corner, login as the device admin:

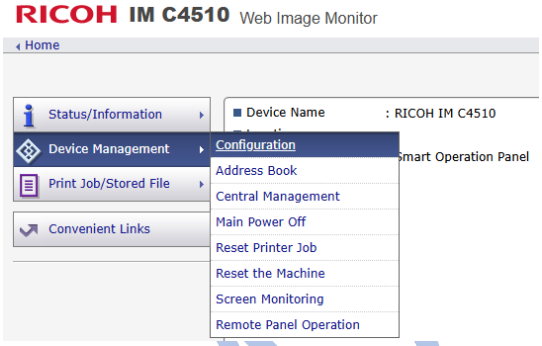


2) Default User Name is admin with no password

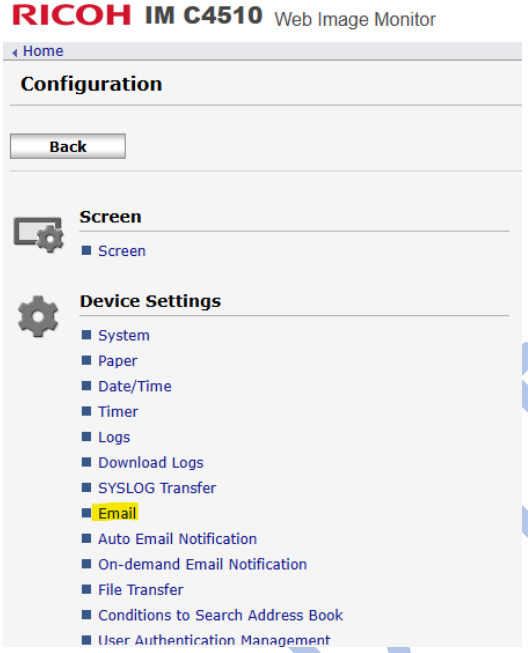


*Note: If this doesn't work, your organization may have changed this, check with your IT or Printer Administrator

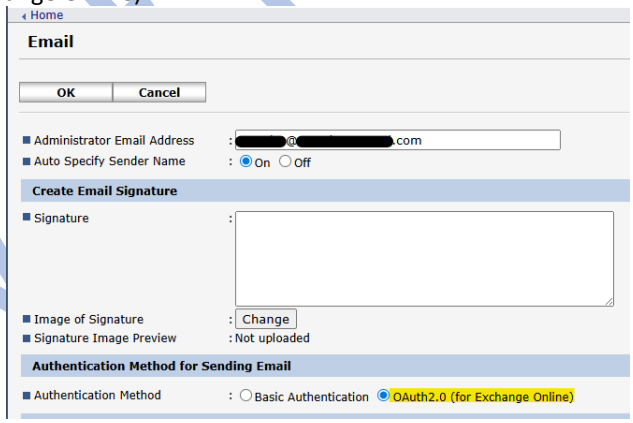
3) Navigate to Device Management>Configuration



4) Select Email under Device Settings

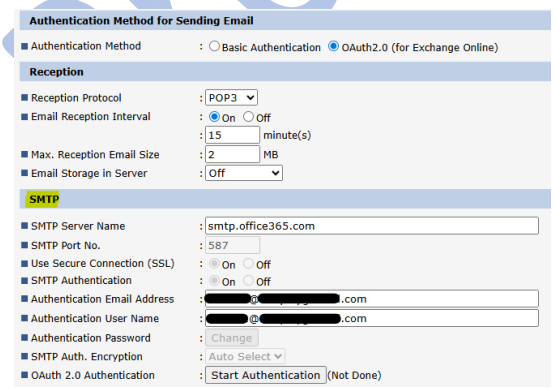


5) Add the scan user that is being used for authentication in the Administrator Email Address at the top. Then under Authentication Method for Sending Email, choose OAuth 2.0 (for Exchange Online)



*Note: If firmware is not up to date or this model is not supported, you will not see this option.

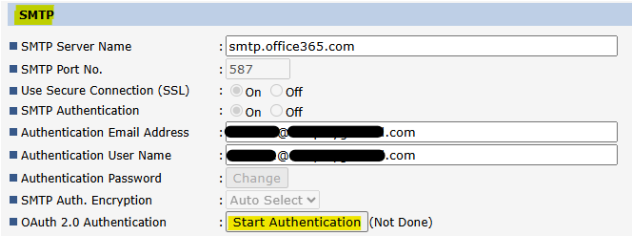
6) In the SMTP Section, the Email & User Name must be a valid email account and the same as the Administrator Email Address as above (if used in the previous step)



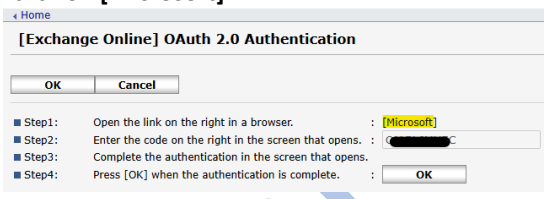
*Note:

SMTP	smtp.office365.com
SMTP Port No.	This will be grayed out – it will use Port 587
Use Secure Connection (SSL)	This will be grayed out – STARTTLS will be used
SMTP Authentication	This will be grayed out – Not used for OAuth 2.0
Authentication Email Address	Enter the email address of the Scan account
Authentication User Name	Enter the email address of the Scan account
Authentication Password	This will be grayed out – Not used for OAuth 2.0
SMPT Auth. Encryption	This will be grayed out – Not used for OAuth 2.0
OAuth 2.0 Authentication	This will say (Not Done)

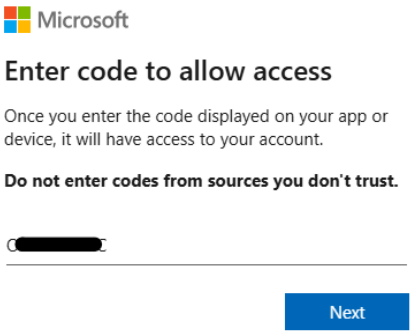
7) Once the Email & User Name is set, select Start Authentication



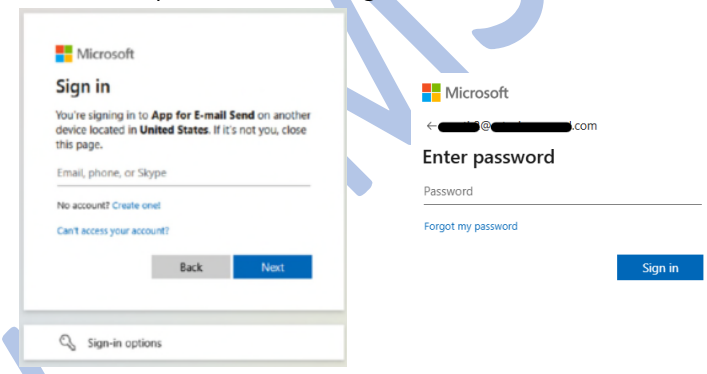
8) Highlight & Copy the code on the right of the screen, then click on **[Microsoft]**



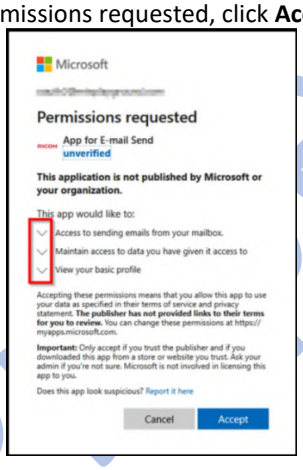
9) Enter the code copied from previous step & click **Next**



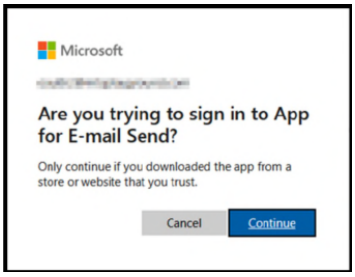
10) Supply the credentials for the Licsensed Scan User account > if this is not the account that is pre-filled, Select + Use another account, and proceed with the sign-in



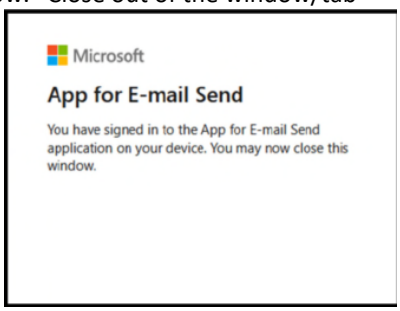
11) Expand each of the dropdowns, and read through the Permissions Requested > if you accept the permissions requested, click **Accept**



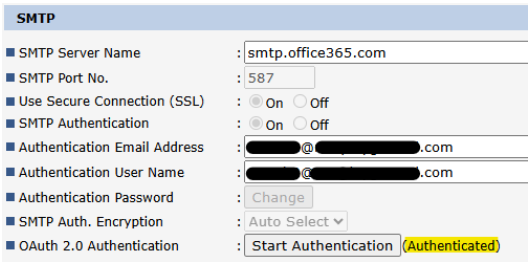
12) Select **Continue**



14) Once you see, “You have signed in to the App for E-mail Send application on your device. You may now close this window.” Close out of the window/tab



15) If done correctly you will see at the bottom next to OAuth 2.0 Authentication, the status has changed to Authenticated

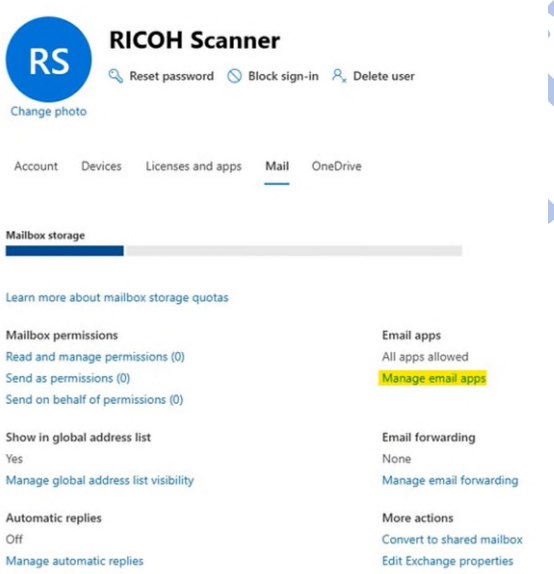


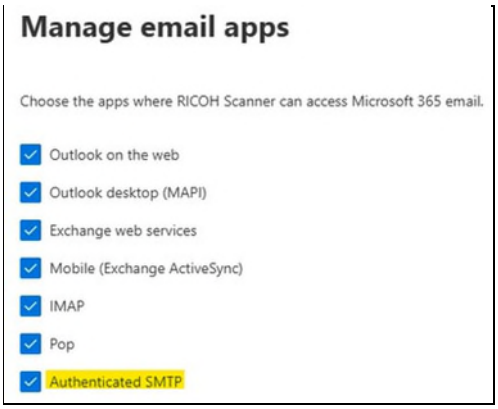
16) Scroll to the top of the screen and click on **[OK]**
17) Test scanning

For a video on how to set this up, please go to: [Ricoh Scanning Resources | Metro Sales Inc]

Troubleshooting

When scanning and get an authentication error, verify these O365 email account settings:

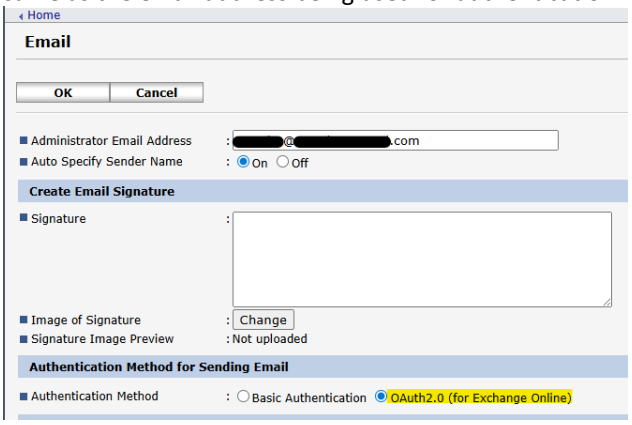




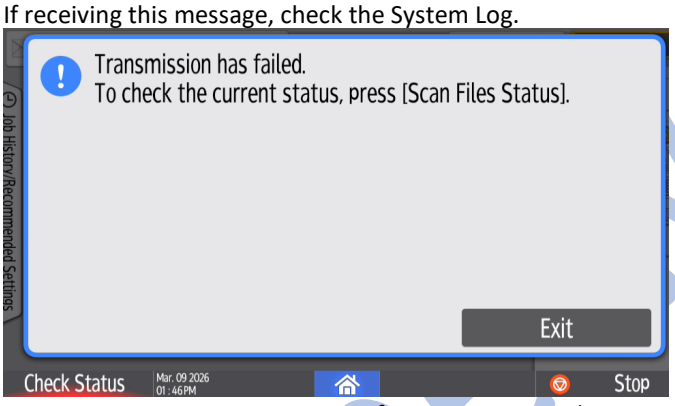
*Note: This can take up to 24 hours to take effect.

Troubleshooting (continued)

If authentication error continues, verify Step 5 above was completed; set the Administrator Email address used is the same as the email address being used for authentication.



If receiving this message, check the System Log.



In WIM>Device Management>Configuration>Network>
System Log:

```
#[dcs_nas(1241)]26/03/09 13:45:23 SMTPC: received error code. [554] (702)  ERR:
#[dcs_nas(1241)]26/03/09 13:45:23 SMTPC: connection closed. (801)  ERR:
```

Verify Firewall is allowing communication from the copier out.

For Microsoft error:
0Auth Authorize Error - AADSTS650051 - Service principal name is already present for the tenant: Wait a minute or two and try again.

Information about this error:
Azure App Registration - 0Auth Authorize Error - AADSTS650051 - Service principal name is already present for the tenant - Microsoft Q&A

Ricoh Statement about Microsoft change:
https://www.ricoh.com/info/2025/0526_1
Microsoft Statement about the change (Microsoft pushed Sept 2025 date to March 2026):
Exchange Online to retire Basic auth for Client Submission (SMTP AUTH) | Microsoft Community Hub
Ricoh guide to setup OAuth 2.0 Authentication:
https://www.ricoh.com/-/Media/Ricoh/Sites/com/info/2025/pdf/0526_1.pdf