

Information and Procedure for enabling OAuth2.0 Scan to Email on a Canon Device

Document Version: 01

Why is this change necessary?

Beginning **March 2026**, Microsoft will permanently disable **Basic Authentication** for **SMTP AUTH** in Exchange Online. This authentication method, which transmits usernames and passwords in plain text, will no longer be supported. As a result, many printers relying on this legacy method for Scan to Email must transition to **OAuth 2.0** or scan via another means.

Will my printers be affected?

Are your printers or print solution configured for Scan to Email and/or Email Notifications?

No Yes

Is your printer or print solution software set to use smtp.office365.com as its SMTP server with authentication enabled?

No Yes

If OAuth2 is not already enabled on your printers or print solution, then they will be affected by the change and remedial action needs to be carried out.

If your printers are not using SMTP authentication, for example they use an on-prem mail server or are sending email unauthenticated via a relay, then you will not be affected by the change, however you may consider switching to OAuth2.0 as a more secure method.

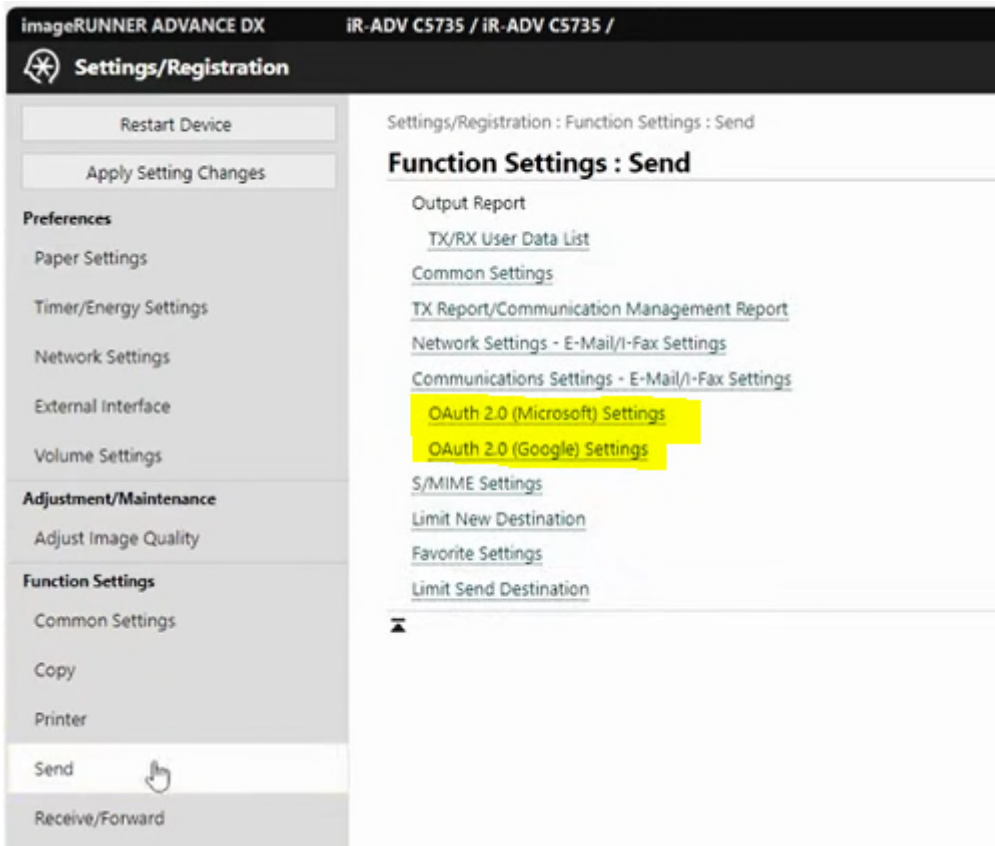
Your printers will not be affected.

Required Firmware

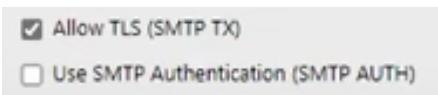
Canon introduced OAuth2 from their DX ranges onwards, unified Firmware Platform (uFP) v3.18 or newer. Fleet MPS have tested on the Canon iR ADV C5550 range, pre-dating the DX range and with a firmware update the OAuth2 settings became available, so we expect to see further updates being released for other older models.

If the settings in the below information do not exist on your device, try updating the firmware via the WebUI, **[Settings / Registration]**, **[License/Other]**, **[Register/Update Software]**, **[Distributed Update]**, **[Confirm New Firmware]**.

Procedure



Click **[Settings/Registration]**, **[Send]**, and note the **OAuth2.0** options



In **[Network Settings - Email / Ifax Settings]**

- Ensure the **SMTP server** is set to: **smtp.office365.com**
- Ensure the **port** is set to **587**
- Ensure **Email Address** is set to the account you wish to send from
- **Enable TLS**, but **leave SMTP Authentication disabled**.

OAuth 2.0 (Microsoft) Settings

Basic Settings Edit...

Use OAuth 2.0 (Microsoft) :	Off
Verify Server Certificate :	Off
Add CN to Verification Items :	Off
Microsoft Entra ID Authorization Server Endpoint :	https://login.microsoftonline.com/organizations/oauth2/v2.0

Server Connection Status
To display the latest registered information, click the update icon for [Last Updated].

Server Connection Status : Not Connected

Information for Authorization
To activate a token, follow the [Message] instructions and perform authorization from [Microsoft Entra ID Authorization Endpoint] before the user code expires. After authorization is complete, do not turn OFF the main power of the device until the token is activated. To display the latest registered information, click the update icon for [Last Updated].

Message : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code HCDZ36RMX to authenticate.

Microsoft Entra ID Authorization Endpoint : https://microsoft.com/devicelogin

User Code : HCDZ36RMX

User Code Expires In : 900 sec.

Token Status
To display the latest registered information, click the update icon for [Last Updated].

Token Status : Not Acquired

Go into [OAuth2.0 (Microsoft) Settings] and press Edit.

Edit Basic Settings

OK Cancel

When [Use OAuth 2.0 (Microsoft)] is set to On, [Display Authentication Screen When Sending] will be disabled and [Information Used for SMTP Server Authentication] will be automatically set to [Device Settings].

Basic Settings

Use OAuth 2.0 (Microsoft)

Verify Server Certificate

Add CN to Verification Items

Microsoft Entra ID Authorization Server Endpoint : https://login.microsoftonline.com/organizations/oauth2/v2.0

Enable **Use Oauth2.0** and set the **server endpoint** as follows:

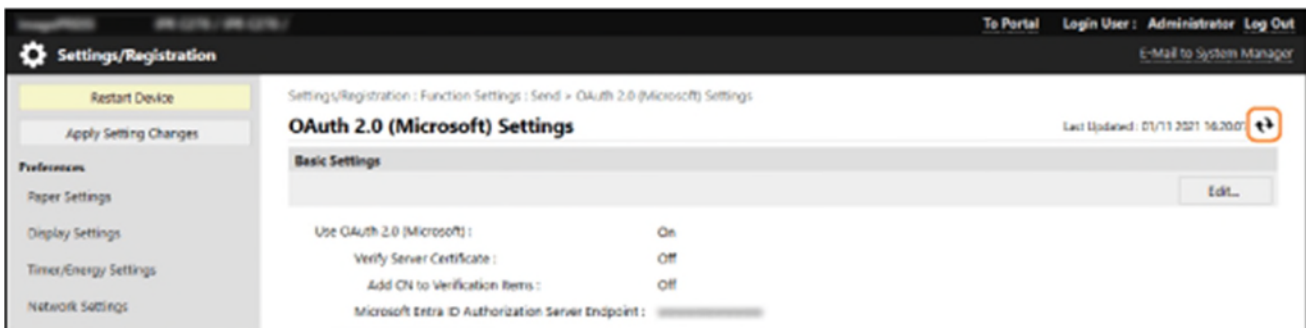
https://login.microsoftonline.com/<tenant>/oauth2/v2.0

Your tenant ID can be found in <https://entra.microsoft.com>, **Overview** under **Basic Information**.

Select whether to verify the certificate when performing TLS encrypted communication with the server.

Click **OK**

Wait for several seconds, and then click the **Refresh** icon



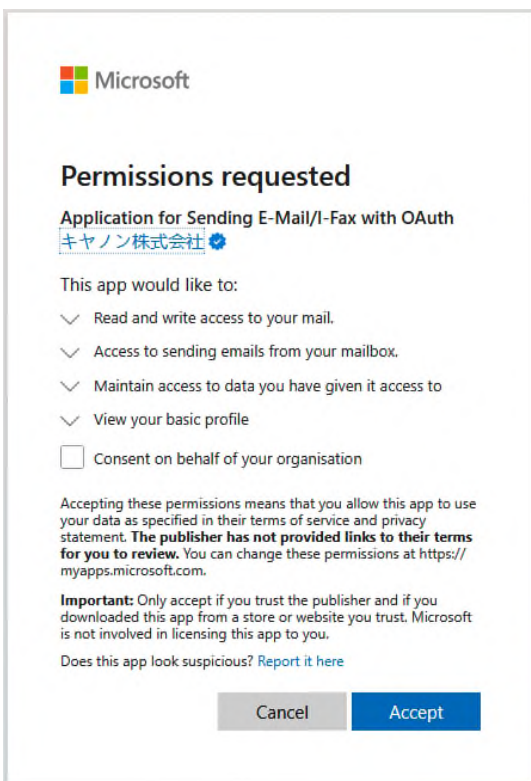
Check that Successfully Connected is displayed for **Server Connection Status**.

OAuth 2.0 (Microsoft) Settings

Last Updated : 08/20/2024 11:13:20 AM ↻

Basic Settings	
Use OAuth 2.0 (Microsoft) :	On
Verify Server Certificate :	Off
Add CN to Verification Items :	Off
Microsoft Entra ID Authorization Server Endpoint :	https://login.microsoftonline.com/organizations/oauth2/v2.0
<p>Server Connection Status</p> <p>To display the latest registered information, click the update icon for [Last Updated].</p> <p>Server Connection Status : Successfully Connected</p>	
<p>Information for Authorization</p> <p>To activate a token, follow the [Message] instructions and perform authorization from [Microsoft Entra ID Authorization Endpoint] before the user code expires. After authorization is complete, do not turn OFF the main power of the device until the token is activated. To display the latest registered information, click the update icon for [Last Updated].</p> <p>Message : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code SZ9SAB76X to authenticate.</p> <p>Microsoft Entra ID Authorization Endpoint : https://microsoft.com/devicelogin</p> <p>User Code : SZ9SAB76X</p> <p>User Code Expires In : 900 sec.</p>	
<p>Token Status</p> <p>To display the latest registered information, click the update icon for [Last Updated].</p> <p>Token Status : Being Acquired...</p>	

Click the link displayed next to **Microsoft Entra ID Authorization Server Endpoint**, and authorize the server according to the instructions on the screen. Beware that the account used for authorization will be the account that email will be sent from.



Follow the instructions entering the user code displayed in **User Code**.

Authorization is performed within the time frame indicated in User Code Expires In.

You will note, that in EntraID, Enterprise Apps, an app is added named “Application for Sending E-Mail/I-Fax with OAuth”.

Troubleshooting

If setup fails, ensure that:

- The printers time and date are set correctly,
- The printer can access the internet (review Gateway, DNS, and Proxy settings),
- Your EntraID account has the appropriate permissions to grant access.