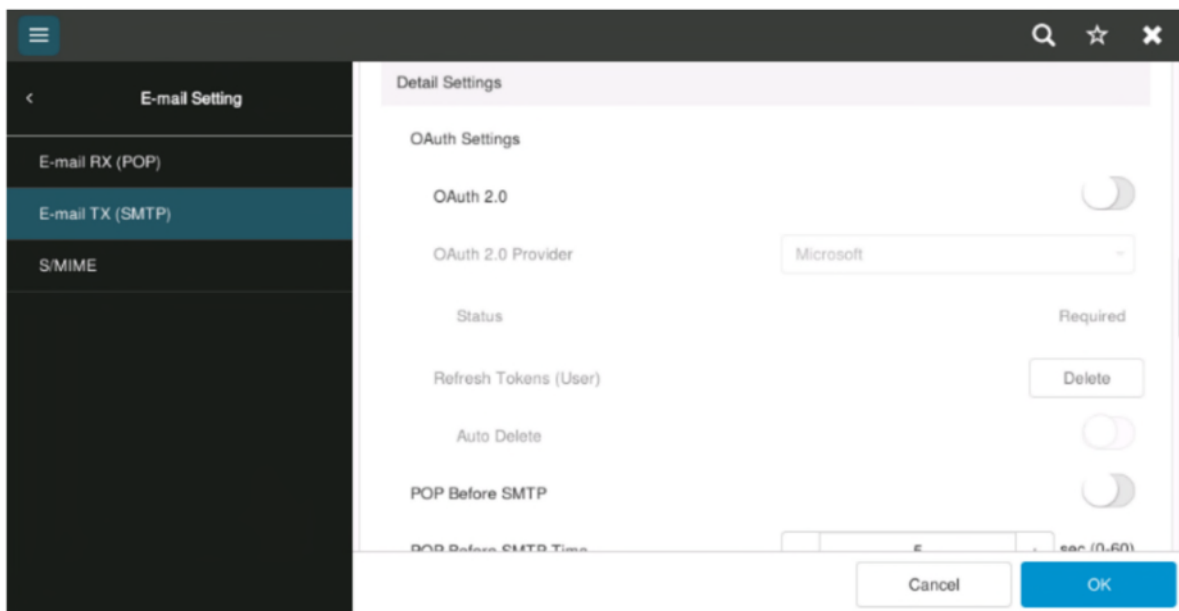# Guide to set up 2.0 authentication Develop

INSTRUCTIONS

1 Step 1: where to find the OAuth Settings (Only via the display, not via the web interface)

Setting screen

[Administrator] > [Network] > [E-mail Setting] > [E-mail TX (SMTP)] > [Detail Settings]

2   Step 2a: Setting "Microsoft" to OAuth 2.0

1.   Set the SSL/TLS version.

Setting screen

[Administrator] > [Security] > [PKI Settings] > [Enable SSL Version] > [SSL/TLS Version Setting]

Setting value

[Minimum TLSv1.2 / Maximum TLS1.2] or [Minimum TLSv1.2 / Maximum TLSv1.3]

Note

If both Minimum and Maximum are set to TLSv1.3, authentication will fail as Microsoft Azure AD service has not yet started supporting TLSv1.3.

2.   Set the administrator and device email addresses

3.	Turn on OAuth 2.0 authentication, then select the OAuth 2.0 provider to Microsoft and touch OK.
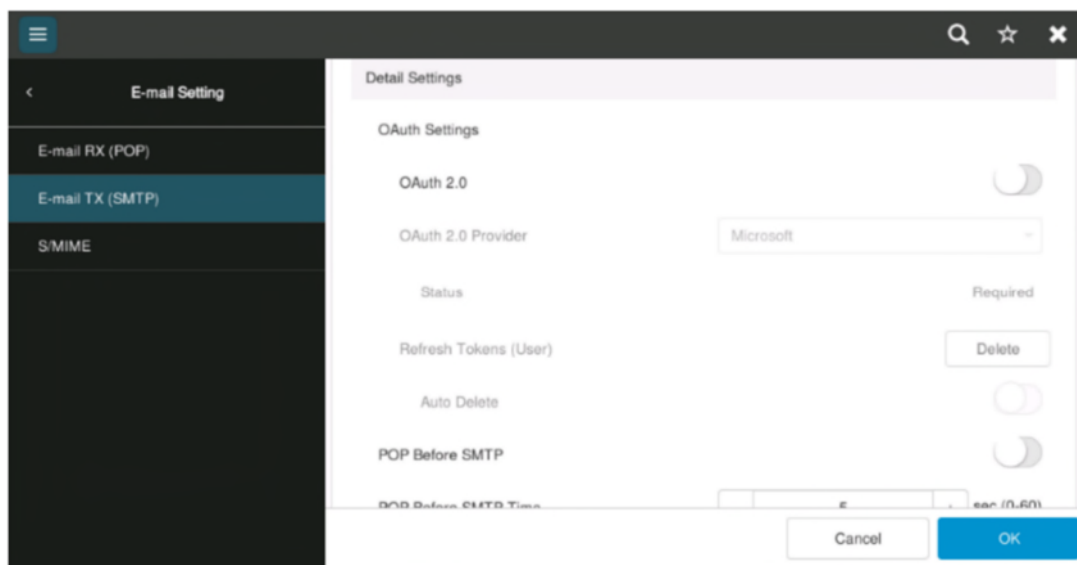
Setting screen

[Administrator] > [Network] > [E-mail settings] > [E-mail sending (SMTP)] > [Detail Settings]

Setting value

OAuth2.0: ON

OAuth2.0 Provider: Microsoft

4.	After touching the OK key in step 3, the Microsoft authentication screen will be displayed.

5.	Enter the password for the administrator address in step 1 to complete the authentication.

6.	Set the SMTP server address to the Microsoft SMTP server name.

Setting screen

[Administrator] > [Network] > [E-mail settings] > [E-mail sending (SMTP)] > [SMTP Server Address]

3   Step 2b: Setting "Google" to OAuth 2.0 (Only via the display, not via the web interface)

1.   Set the WebDAV TX setting to ON.

Setting screen

[Administrator] > [Network] > [WebDAV Settings] > [WebDAV Client Settings] > [WebDAV TX Setting]

Remarks

When Google is selected in Cloud service provider setting, WebAPI/WebDAV will be used for the communication with Google server. WebDAV TX setting must be ON consequently.

Depending on the size of the scanned file, a timeout may occur on sending the file. Please set a longer connection timeout in the WebDAV client settings in that case.

The recommended setting for the connection timeout is 120 seconds or longer.

When the timeout happens, Server connection error will occur, and the job will be deleted.

The maximum file size that can be sent by Gmail is 25MB.

2.   Set the SSL/TLS version.

Setting screen

[PageScope Web Connection] > [Administrator] > [Security] > [PKI Settings] > [Enable SSL Version] > [SSL/TLS Version Setting]

Setting value

[Minimum TLSv1.2 / Maximum TLS1.2], [Minimum TLSv1.2 / Maximum TLSv1.3] or [Minimum TLSv1.3 / Maximum TLSv1.3]

Note

If set to [Minimum TLSv1.3 / Maximum TLSv1.3], please set the HTTP version to "HTTP/2, HTTP/1.1".

Setting screen

[Administrator] > [Network] > [WebDAV Settings] > [WebDAV Client Settings] >

[Certificate Verification Level Settings] > [HTTP Version Setting]

When TLSv1.3 is used, Google's server will request SNI information. In order to respond to that request, the WebDAV client must be configured to use HTTP/2 in HTTP Version Setting.

3.   Set the administrator and device email addresses.

4.   Turn on OAuth 2.0 authentication, then select the OAuth 2.0 provider to Google and touch OK.

Setting screen

[Administrator] > [Network] > [E-mail settings] > [E-mail sending (SMTP)] > [Detail Settings]

Setting value

OAuth2.0: ON

OAuth2.0 Provider: Google

5.   After touching the OK key in step 4, the Google authentication screen will be displayed.

6.   Enter the password for the administrator address in step 3 to complete the authentication.
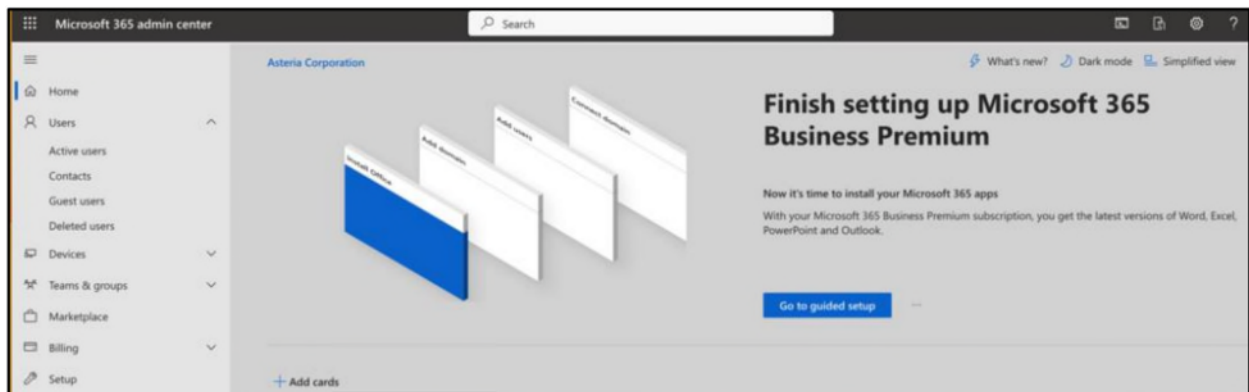
Troubleshooting

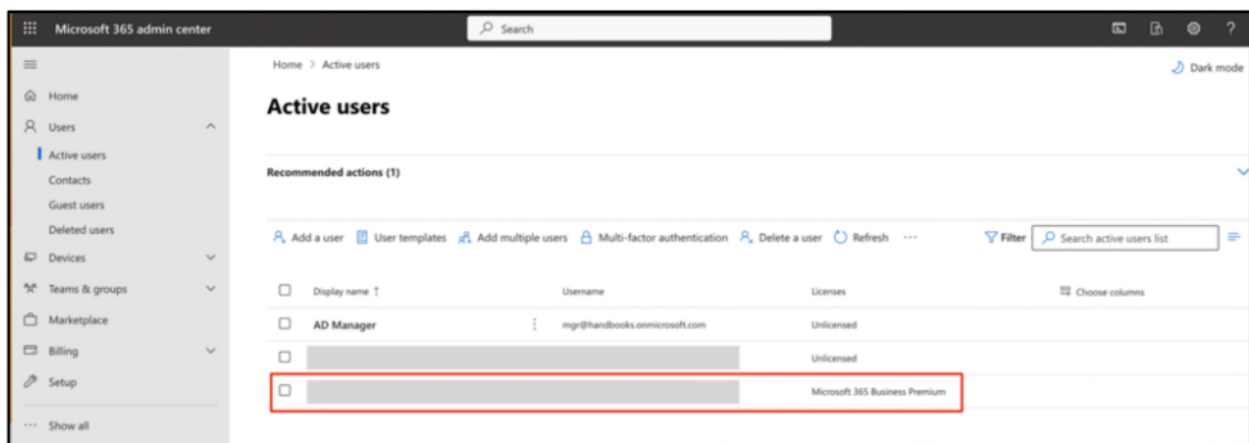ScanToEmail fails with error code 535 when the OAuth2.0 provider is Microsoft.

Please check that the authenticated SMTP setting is enabled in the Microsoft 365 Management center.
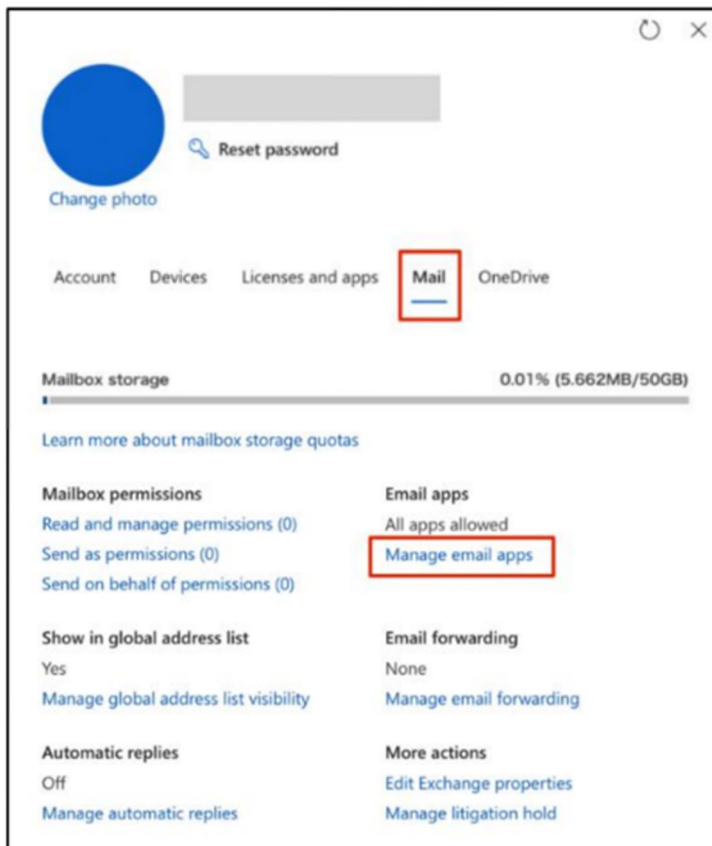
[Procedure]

1. Open Microsoft 365 Management Center.

2. Select Active Users from the left menu

3.	Select Active Users from the left menu

4.	Please enable authenticated SMTP and save it. The set contents may not be reflected immediately, so if the same error continues to occur in sending mail, please try again after a while. If the error continues to occur, please check the settings again.