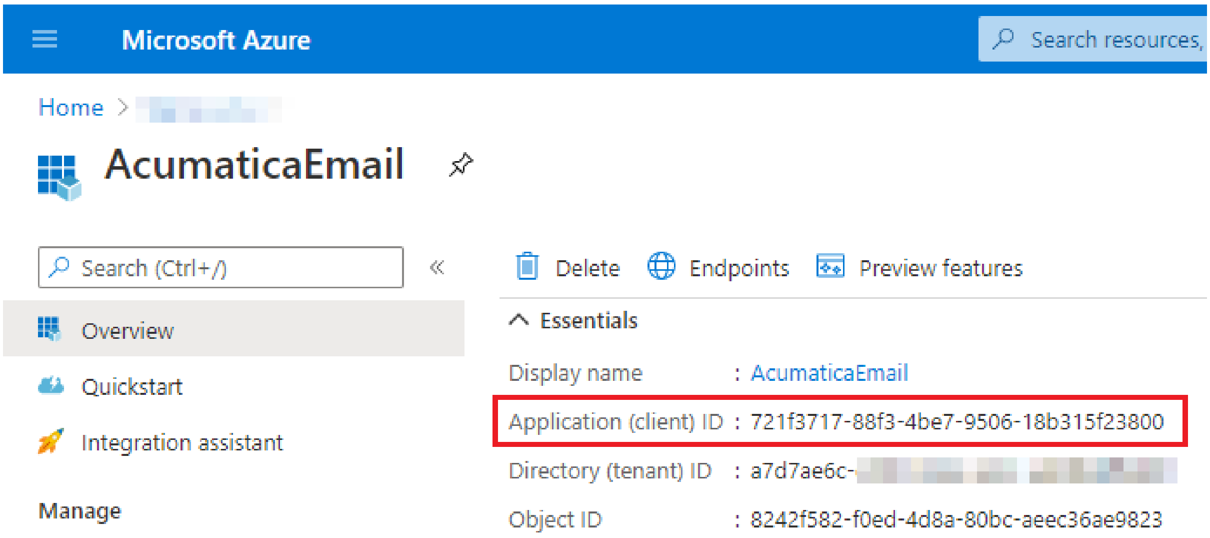
A. System Email Account

Step 1: On the [Microsoft Azure Portal](), complete steps from the [Register an application with the Microsoft identity platform]() section. On the Overview page, copy the following values which will be used in the MYOB setup:

- Application (client) ID
- Directory (tenant) ID

The example of these values is shown in the following screenshots.

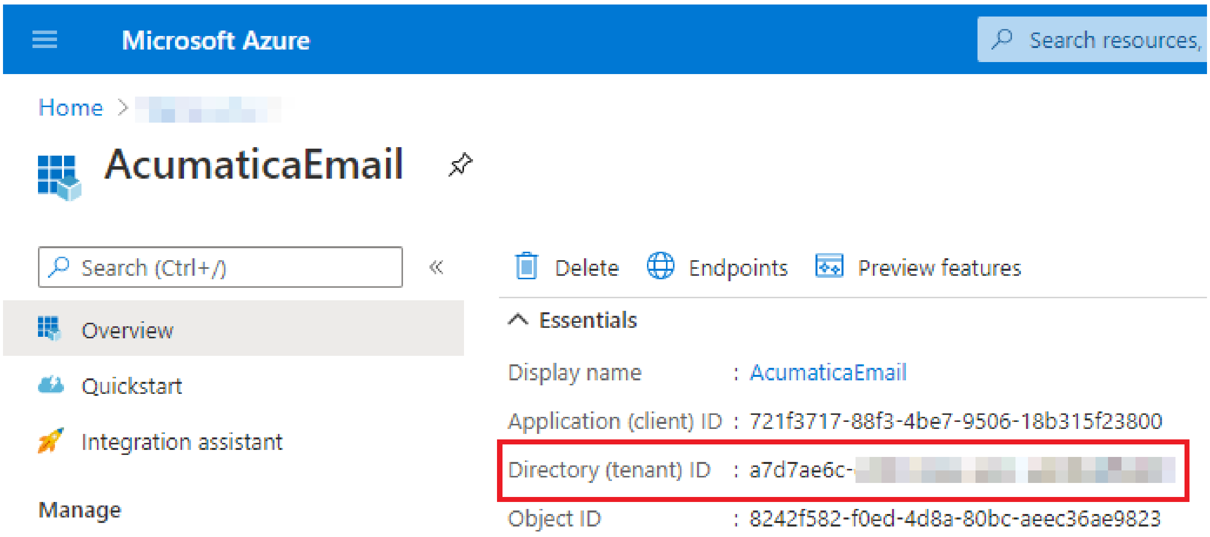


Display name : AcumaticaEmail

Application (client) ID : 721f3717-88f3-4be7-9506-18b315f23800

Directory (tenant) ID : a7d7ae6c-[redacted]

Object ID : 8242f582-f0ed-4d8a-80bc-aeec36ae9823



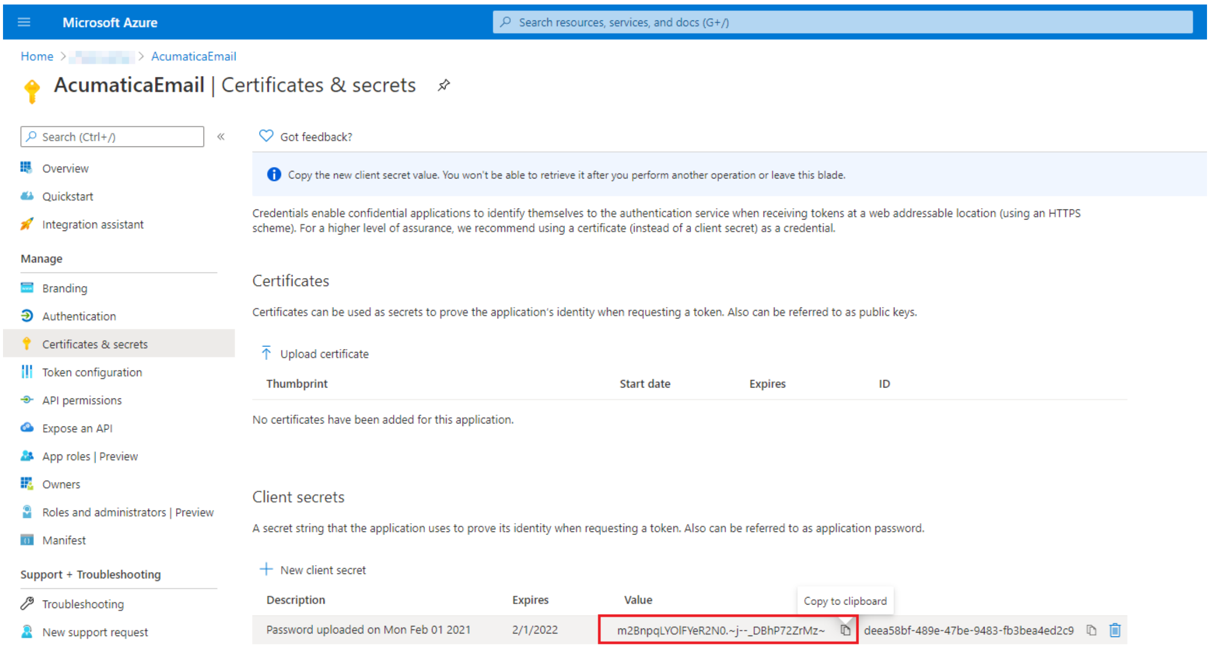
Display name : AcumaticaEmail

Application (client) ID : 721f3717-88f3-4be7-9506-18b315f23800

Directory (tenant) ID : a7d7ae6c-[redacted]

Object ID : 8242f582-f0ed-4d8a-80bc-aeec36ae9823

Step 2: On Microsoft Azure Portal, complete steps from the [Add a client secret for an application]() section. Copy the client secret value shown in the following screenshot. The value will be used in the MYOB setup.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > [redacted] > AcumaticaEmail

AcumaticaEmail | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

Client secrets

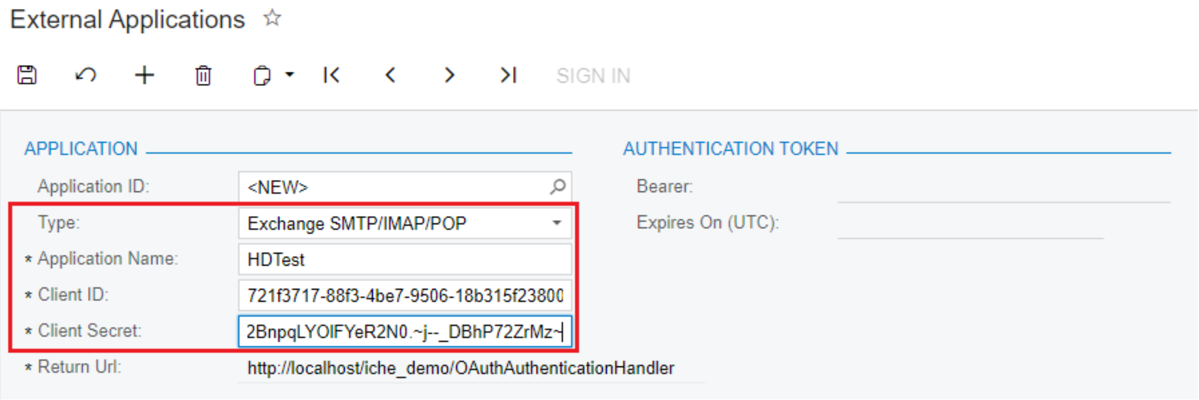
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	
Password uploaded on Mon Feb 01 2021	2/1/2022	m2BnpqLYOlFYeR2N0.~j--_DBhP72ZrMz~	deea58bf-489e-47be-9483-fb3bea4ed2c9

Step 3: In MYOB, on the External Applications (SM301000) form, create a new record by doing the following:

1. In the **Type** drop down, select the *Exchange SMTP/IMAP/POP* value.
2. In the Application **Name** box, specify the application name.
3. In the **Client ID** box, specify the *Application (client) ID* value from **Step 1**.
4. In the **Client Secret** box, specify the *Client secret* value from **Step 2**.
5. Save your changes.

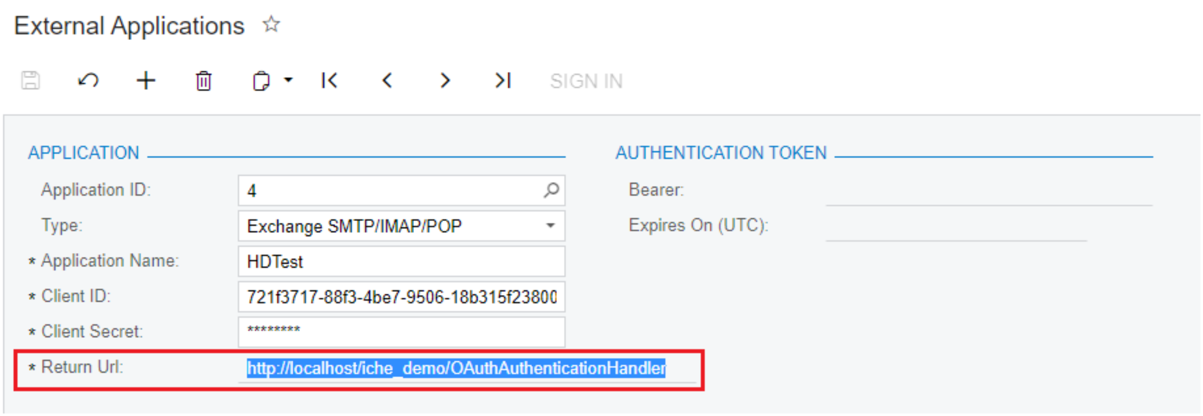
The specified values are shown in the following screenshot.



External Applications ☆

Application ID:	<NEW>
Type:	Exchange SMTP/IMAP/POP
* Application Name:	HDTest
* Client ID:	721f3717-88f3-4be7-9506-18b315f23800
* Client Secret:	2BnpqLYOIFYeR2N0.~j--_DBhP72ZrMz~
* Return Url:	http://localhost/iche_demo/OAuthAuthenticationHandler
Bearer:	
Expires On (UTC):	

Step 4: Copy the value from the Return URL box. The value will be used in the next step for the Azure application setup.



External Applications ☆

SIGN IN

APPLICATION

Application ID: 4

Type: Exchange SMTP/IMAP/POP

* Application Name: HDTest

* Client ID: 721f3717-88f3-4be7-9506-18b315f23800

* Client Secret: ********

* Return Url: http://localhost/iche_demo/OAuthAuthenticationHandler

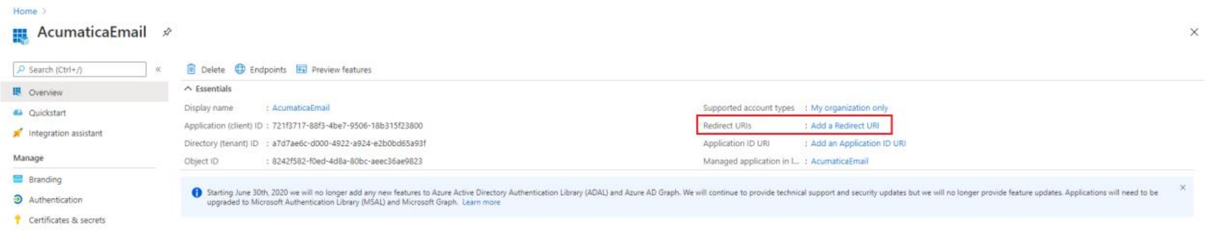
AUTHENTICATION TOKEN

Bearer:

Expires On (UTC):

Step 5: On the Microsoft Azure Portal, complete steps from the Add a redirect URI section as follows:

1. On the Overview page, click the **Add a Redirect URI** link as shown in the following screenshot



Home >

AcumaticaEmail

Essentials

Display name : AcumaticaEmail

Application (client) ID : 721f3717-88f3-4be7-9506-18b315f23800

Directory (tenant) ID : a7d7ae6c-d000-4922-a924-e2b0bd65a93f

Object ID : 8242f582-f0ed-4d8a-80bc-aeec36ae9823

Supported account types : My organization only

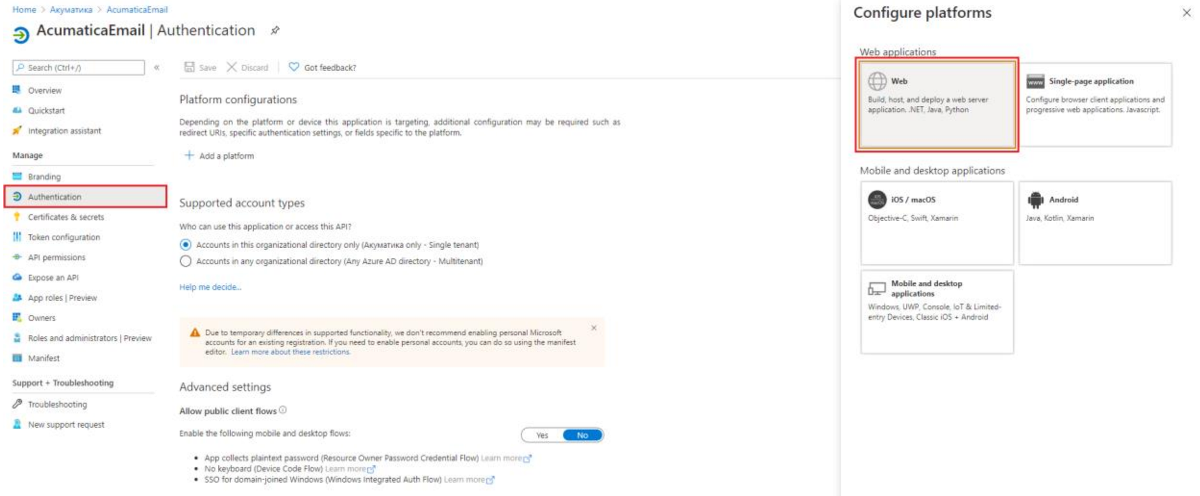
Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in l... : AcumaticaEmail

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

2. In Configure platforms, select the Web tile as shown in the following screenshot



Home > Акуматика > AcumaticaEmail

AcumaticaEmail | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Акуматика only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Configure platforms

Web applications

Web Build, host, and deploy a web server application. .NET, Java, Python

Single-page application Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications

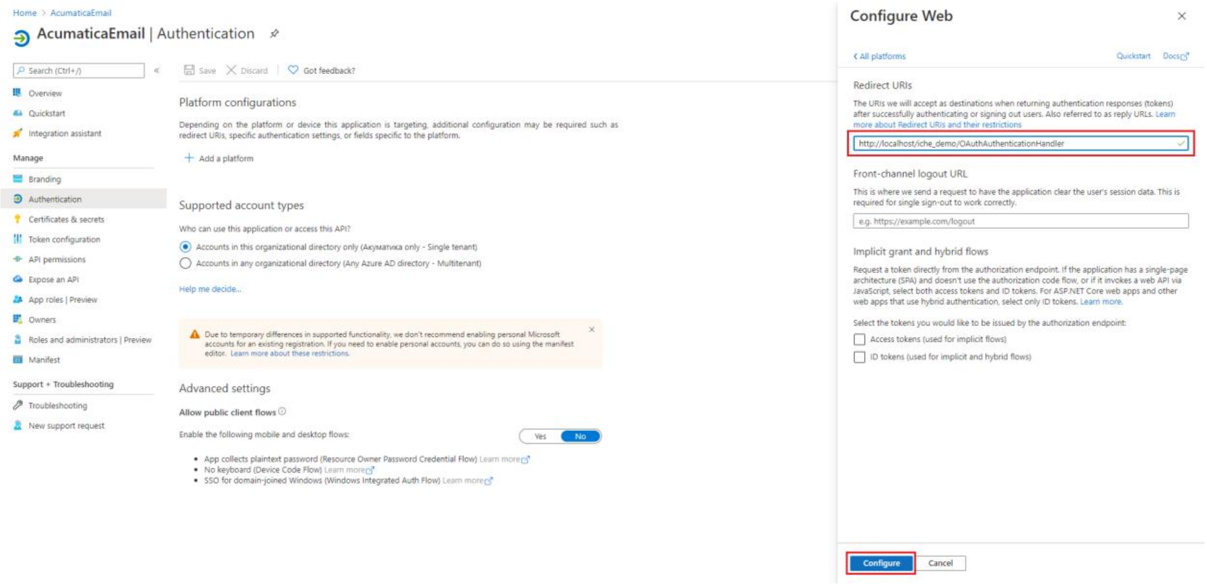
iOS / macOS Objective-C, Swift, Xamarin

Android Java, Kotlin, Xamarin

Mobile and desktop applications Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

3. In the **Redirect URI** box, specify the **Return URL** box value from **Step 4**.
4. Click the **Configure** button.

The following screenshot demonstrates instructions 3 and 4.



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Акуматика only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

http://localhost/iche_demo/OAuthAuthenticationHandler

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more.

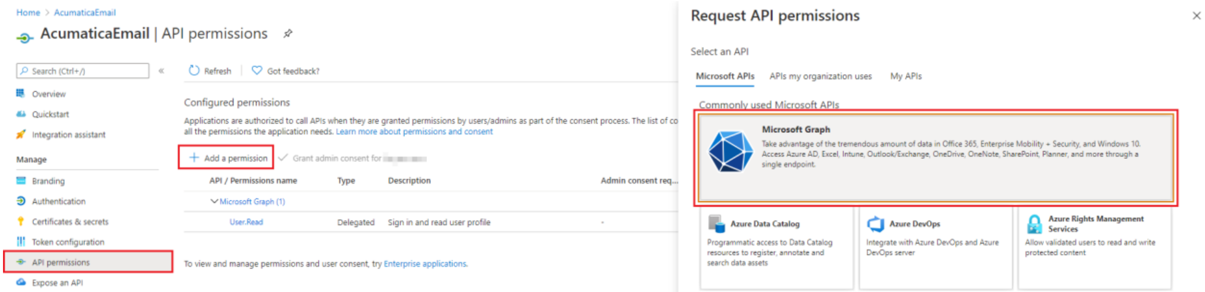
Select the tokens you would like to be issued by the authorization endpoint:

□ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

Step 6: On the Microsoft Azure Portal, complete steps from Application permission to Microsoft Graph to grant the needed delegated permissions as follows:

1. Select **API permissions > Add a permission > Microsoft Graph** as the following screenshot shows.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

To view and manage permissions and user consent, try Enterprise applications.

Select an API

Commonly used Microsoft APIs

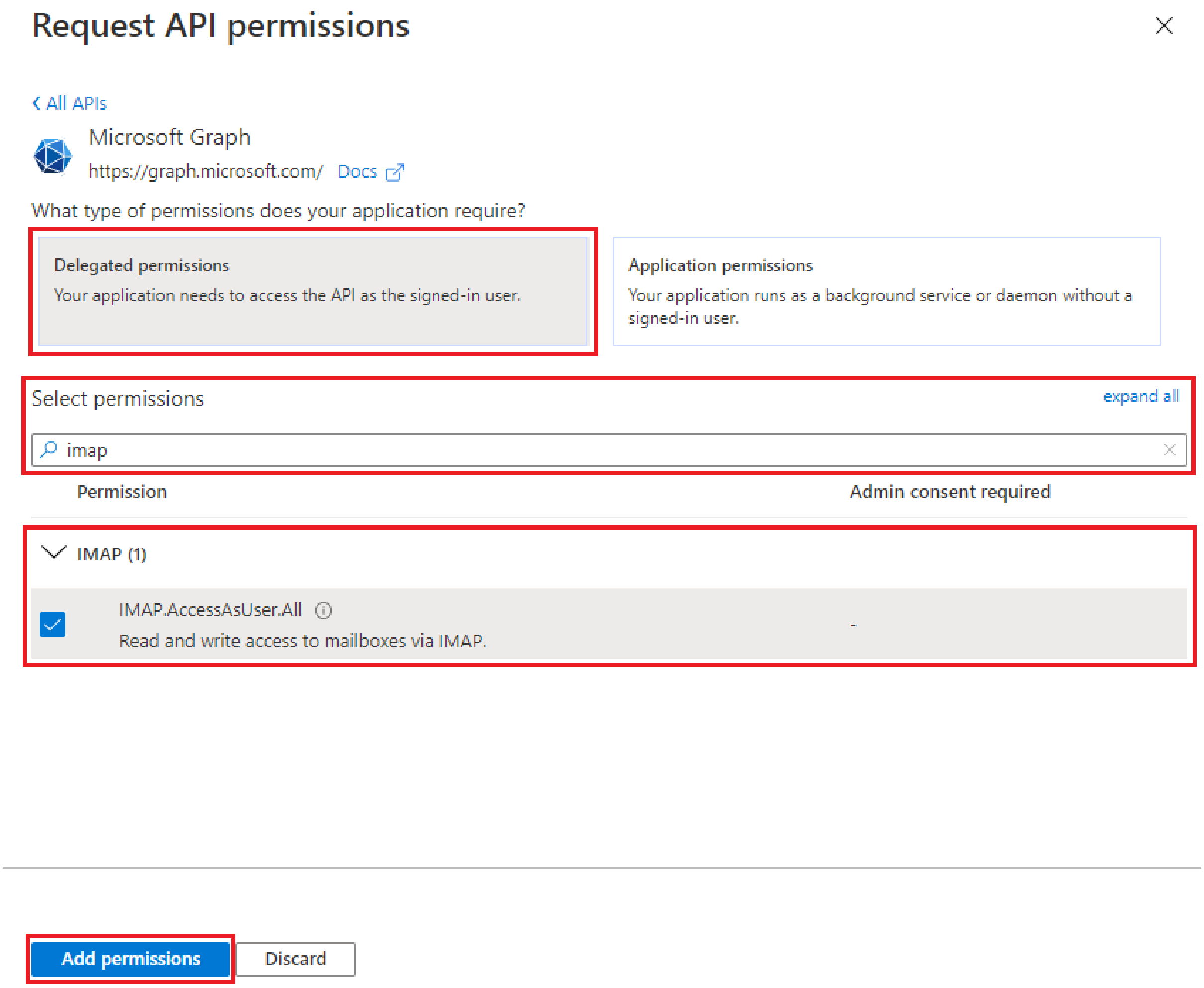
Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

2. Select **Delegated permissions**.
3. Select the following permissions:
    1. *offline_access*
    2. *IMAP.AccessAsUser.All*
    3. *SMTP.Send*
    4. *POP.AccessAsUser.All* if needed (however, using POP3 not recommended in Acumatica in general)
4. Click **Add Permissions** button as shown in the following screenshot.



Request API permissions

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

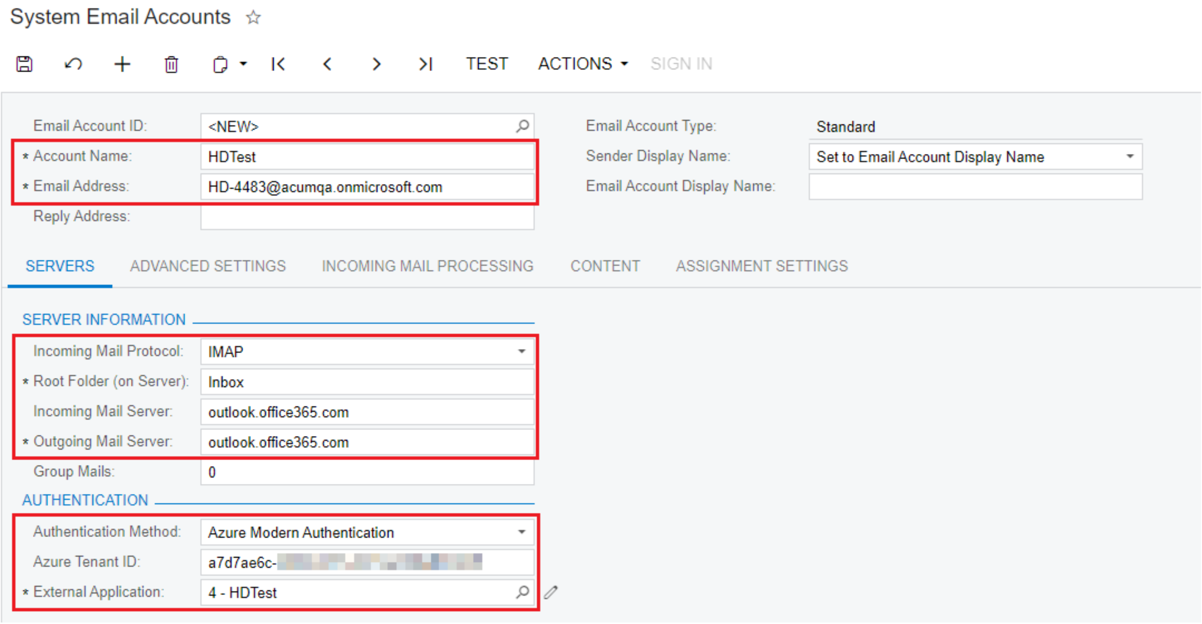
imap

Permission	Admin consent required
IMAP (1)	
☑ IMAP.AccessAsUser.All Read and write access to mailboxes via IMAP.	-

Step 7: In MYOB, on the System Email Account (SM204002) form, create a new record.

a. On the **Servers** tab, specify the following values:
   1. In the **Account Name** box, specify the account name.
   2. In the **Email Address** box, specify the email address.
   3. Select the **Incoming Mail Protocol** needed.
   4. Specify the **Root Folder** box value.
   5. Specify the **Incoming Mail Server** and **Outgoing Mail Server** boxes values (*outlook.office365.com* for Azure/Office365).
   6. In the **Authentication Method** drop down, select the *Azure Modern Authentication (OAuth 2.0)* option.
   7. In the **Azure Tenant ID** box, specify the *Directory (tenant) ID* value from **Step 1**.
   8. In the **External Application** box, select the external application created in **Step 3**.

Example is shown in the following screenshot.



System Email Accounts ☆

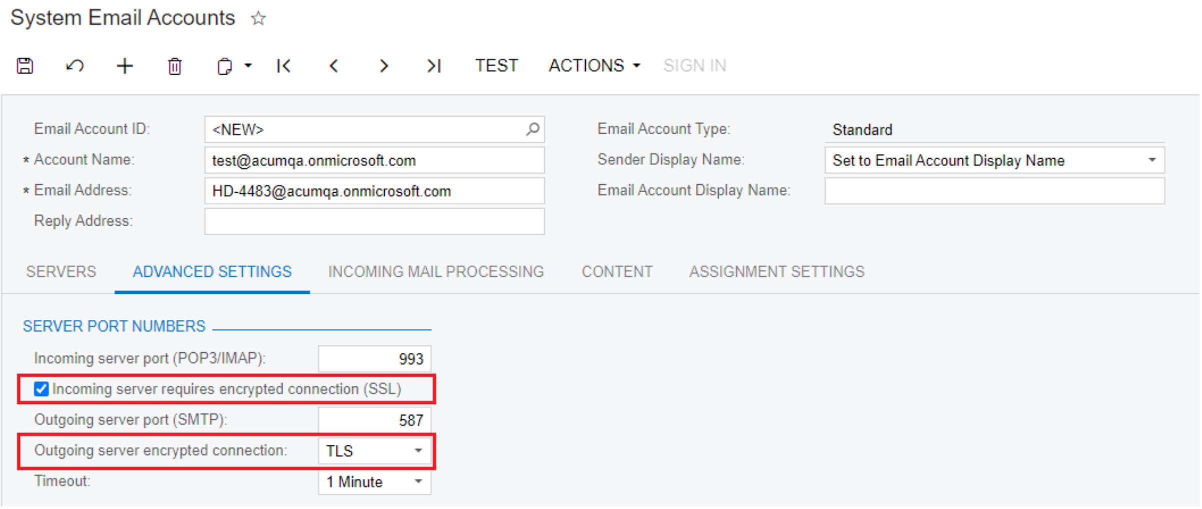
Email Account ID: <NEW>
* Account Name: HDTest
* Email Address: HD-4483@acumqa.onmicrosoft.com
Reply Address:
Email Account Type: Standard
Sender Display Name: Set to Email Account Display Name
Email Account Display Name:

SERVER INFORMATION
Incoming Mail Protocol: IMAP
* Root Folder (on Server): Inbox
Incoming Mail Server: outlook.office365.com
* Outgoing Mail Server: outlook.office365.com
Group Mails: 0

AUTHENTICATION
Authentication Method: Azure Modern Authentication
Azure Tenant ID: a7d7ae6c-[redacted]
* External Application: 4 - HDTest

b. On the **Advanced Settings** tab, specify the following values:
   1. If your server supports the encrypted incoming connection, select the **Incoming server requires encrypted connection (SSL)** check box.
   2. If your server supports the encrypted outgoing connection, select the *TLS* option on the **Outgoing server encrypted connection**.

The tab is shown in the following screenshot.



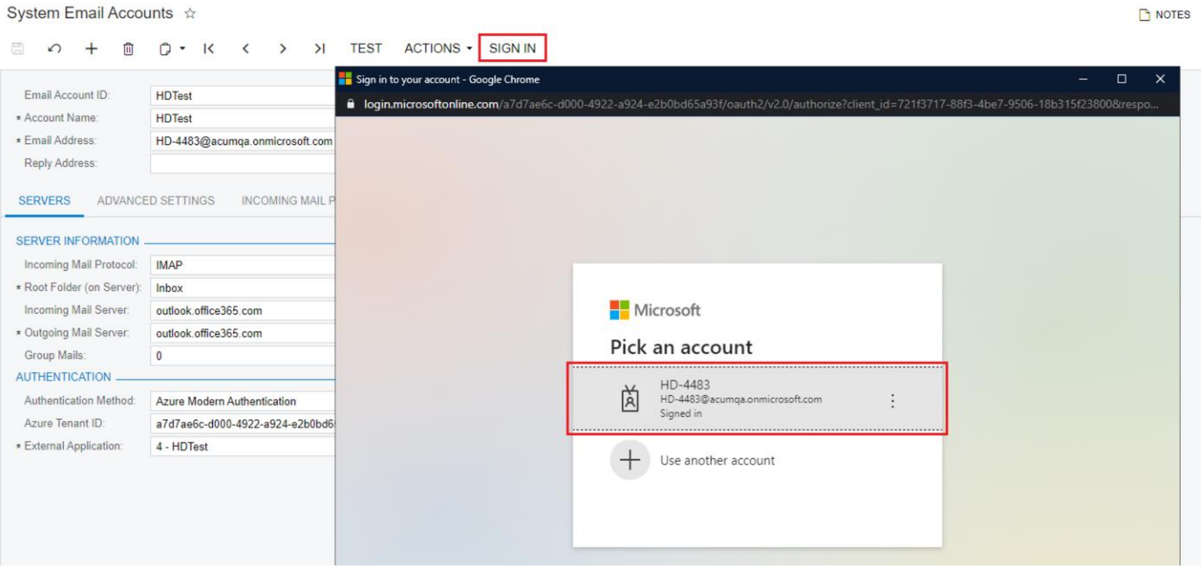
System Email Accounts ☆

Email Account ID: <NEW>
* Account Name: test@acumqa.onmicrosoft.com
* Email Address: HD-4483@acumqa.onmicrosoft.com
Reply Address:
Email Account Type: Standard
Sender Display Name: Set to Email Account Display Name
Email Account Display Name:

SERVER PORT NUMBERS
Incoming server port (POP3/IMAP): 993
☑ Incoming server requires encrypted connection (SSL)
Outgoing server port (SMTP): 587
Outgoing server encrypted connection: TLS
Timeout: 1 Minute

c. **Save your changes.**

Step 8: Click the Sign In button. On the Sign into your account pop up page opened, select and sign into your email account as shown in the following screenshot.



Email Account ID: HDTest
* Account Name: HDTest
* Email Address: HD-4483@acumqa.onmicrosoft.com
Reply Address:

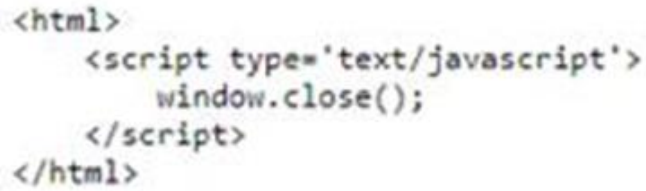
SERVER INFORMATION
Incoming Mail Protocol: IMAP
* Root Folder (on Server): Inbox
Incoming Mail Server: outlook.office365.com
* Outgoing Mail Server: outlook.office365.com
Group Mails: 0

AUTHENTICATION
Authentication Method: Azure Modern Authentication
Azure Tenant ID: a7d7ae6c-d000-4922-a924-e2b0bd6
* External Application: 4 - HDTest

Sign in to your account - Google Chrome
login.microsoftonline.com/a7d7ae6c-d000-4922-a924-e2b0bd65a93f/oauth2/v2.0/authorize?client_id=721f3717-88f3-4be7-9506-18b315f23800&respo...

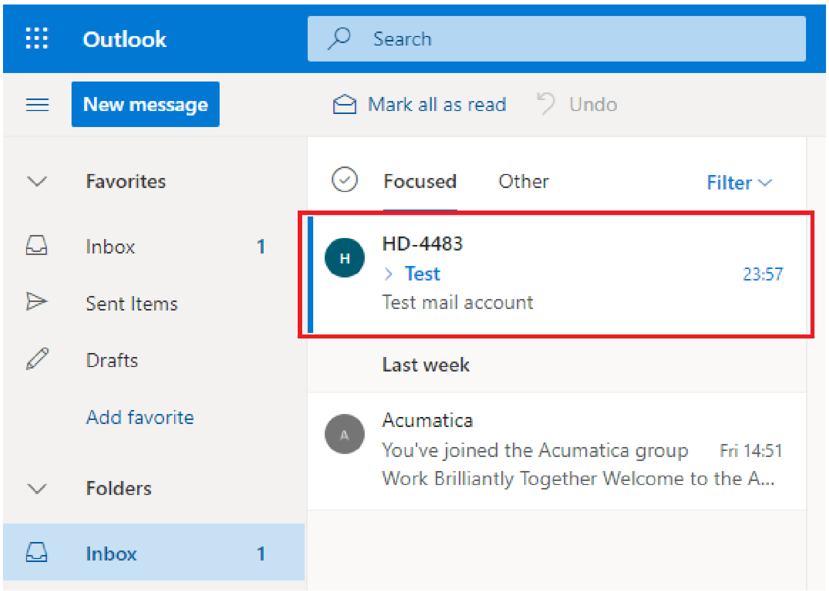
Microsoft
Pick an account
HD-4483
HD-4483@acumqa.onmicrosoft.com
Signed in
Use another account

- The **Sign in** button will request your email address, password and 2FA code, if enabled for your account.
- After successfully signing in, you should have a short notice when it was successfully signed in otherwise a long-detailed error if it has failed. Short notice would be like below **-**



```
<html>
    <script type='text/javascript'>
        window.close();
    </script>
</html>
```

Step 9: Click the Test button to send a test email to your email account. *When you have successfully tested the email, it should give you a green box, indicated it has been completed otherwise a red warning or error if it has failed*. Verify the test email in your inbox folder. Example is shown in the following screenshot.



HD-4483
Test 23:57
Test mail account

Last week

Acumatica
You've joined the Acumatica group Fri 14:51
Work Brilliantly Together Welcome to the A...

Results

The system email account is set up using the Modern Authentication (OAuth 2.0).

B. Exchange Integration

Step-by-step guide

Step 1: On the Microsoft Azure Portal, complete steps from the Register an application with the Microsoft identity platform section. On the Overview page, copy the following values which will be used in the MYOB setup:

- Application (client) ID
- Directory (tenant) ID

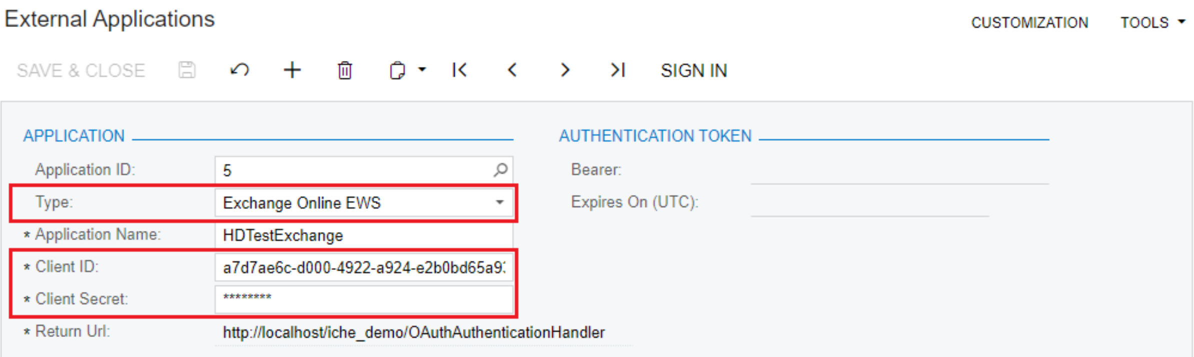
Step 2: On Microsoft Azure Portal, complete steps from the Add a client secret for an application section. Copy the client secret value shown in the following screenshot. The value will be used in the MYOB setup.

Step 3: In MYOB, create an external application and add a redirect url in Microsoft Azure portal.

a. In MYOB, create an the External Applications (SM301000) form, create a new record by doing the following:
   1. In the Type drop down, select the *Exchange Online EWS* value.
   2. In the **Application Name** box, specify the application name needed.
   3. In the **Client ID** box, specify the *Application (client) ID* value from **Step 1**.

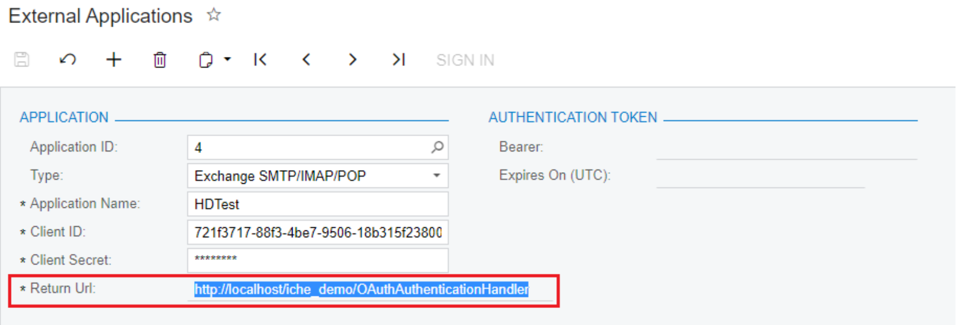
4. In the **Client Secret** box, specify the *Client secret* value from Step 2.
5. Save your changes.

Example is shown in the following screenshot.



Application ID: 5
Type: Exchange Online EWS
* Application Name: HDTestExchange
* Client ID: a7d7ae6c-d000-4922-a924-e2b0bd65a9:
* Client Secret: ********
* Return Url: http://localhost/iche_demo/OAuthAuthenticationHandler
Bearer:
Expires On (UTC):

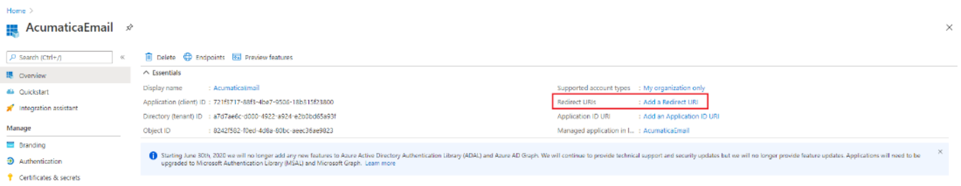
b. Copy the value from the **Return Url** field. The value will be used in the next step for the Azure application setup.



Application ID: 4
Type: Exchange SMTP/IMAP/POP
* Application Name: HDTest
* Client ID: 721f3717-88f3-4be7-9506-18b315f23800
* Client Secret: ********
* Return Url: http://localhost/iche_demo/OAuthAuthenticationHandler
Bearer:
Expires On (UTC):

c. On the Microsoft Azure Portal, complete steps from the **Add a redirect URI** section as follows:

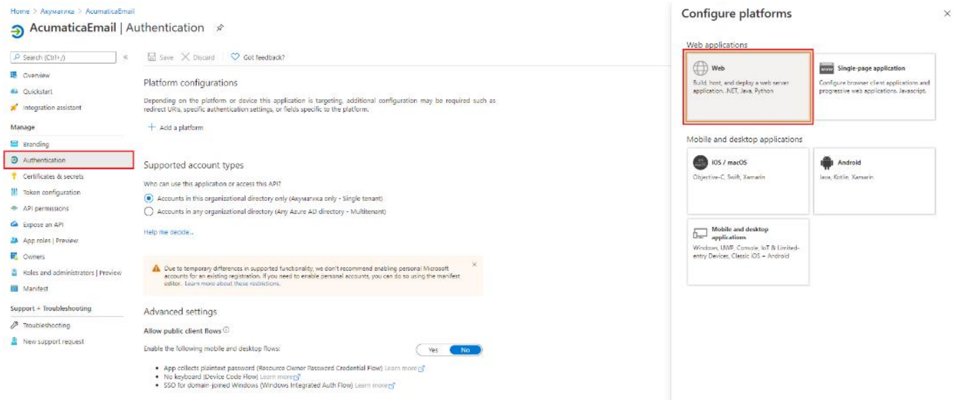
1. On the Overview page, click the **Add a Redirect URI l**ink as shown in the following screenshot



Display name : AcumaticaEmail
Application (client) ID : 721f3717-88f3-4be7-9506-18b315f23800
Directory (tenant) ID : a7d7ae6c-d000-4922-a924-e2b0bd65a93f
Object ID : 8242f582-f0ed-4d8a-80bc-aeec36ae9823
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : AcumaticaEmail

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

2. In **Configure** platforms, select the **Web** tile as shown in the following screenshot



Home > Акуматика > AcumaticaEmail

AcumaticaEmail | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Акуматика only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Configure platforms

Web applications

Web Build, host, and deploy a web server application. .NET, Java, Python

Single-page application Configure browser client applications and progressive web applications. Javascript.

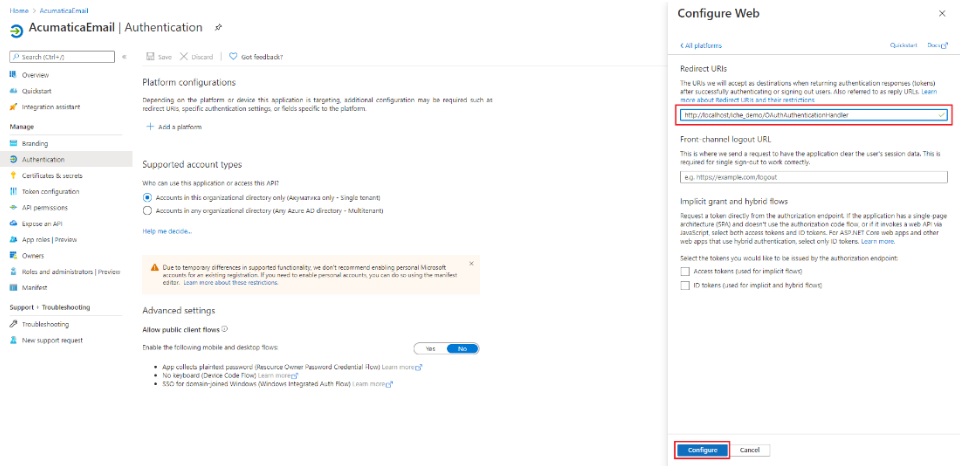
Mobile and desktop applications

iOS / macOS Objective-C, Swift, Xamarin

Android Java, Kotlin, Xamarin

Mobile and desktop applications Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

3. In the **Redirect URI** box, specify the Return URL box value from Step 3 below.



Home > AcumaticaEmail

AcumaticaEmail | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Акуматика only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: Yes [✓ No]

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Configure Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

http://localhost/ichē_demo/OAuthAuthenticationHandler

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more.

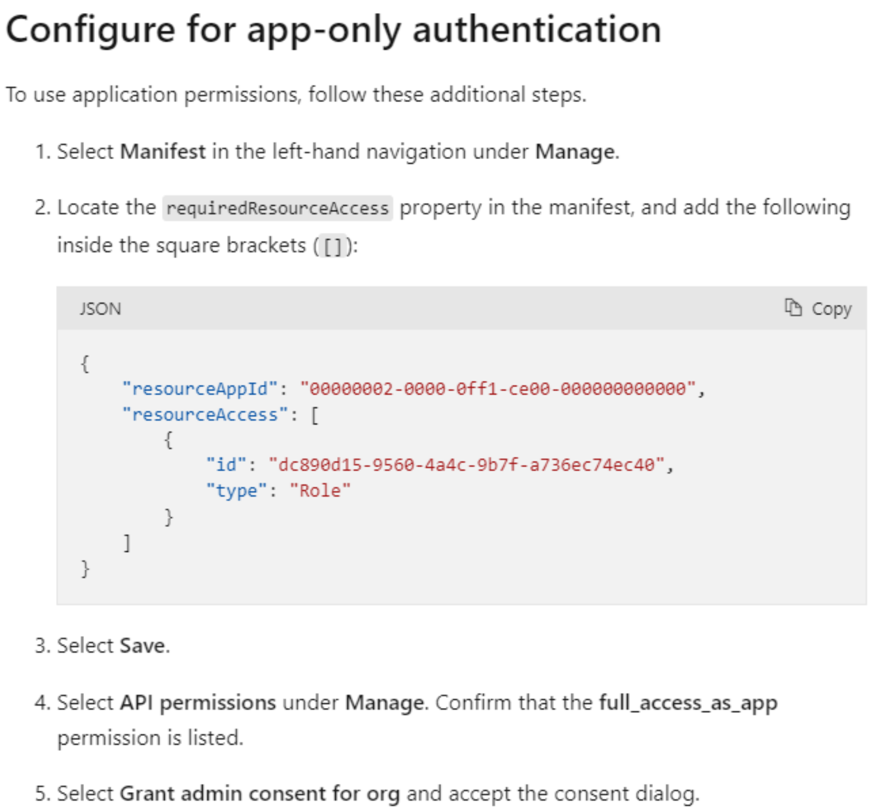
Select the tokens you would like to be issued by the authorization endpoint:

□ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

4. Click the **Configure** button.

Step 4: On the Microsoft Azure Portal, complete steps from [Configure for app-only authentication]() to grant the delegated permissions. This will guide you to update the Manifest.



Configure for app-only authentication

To use application permissions, follow these additional steps.

1. Select **Manifest** in the left-hand navigation under **Manage**.
2. Locate the `requiredResourceAccess` property in the manifest, and add the following inside the square brackets (`[]`):

JSON

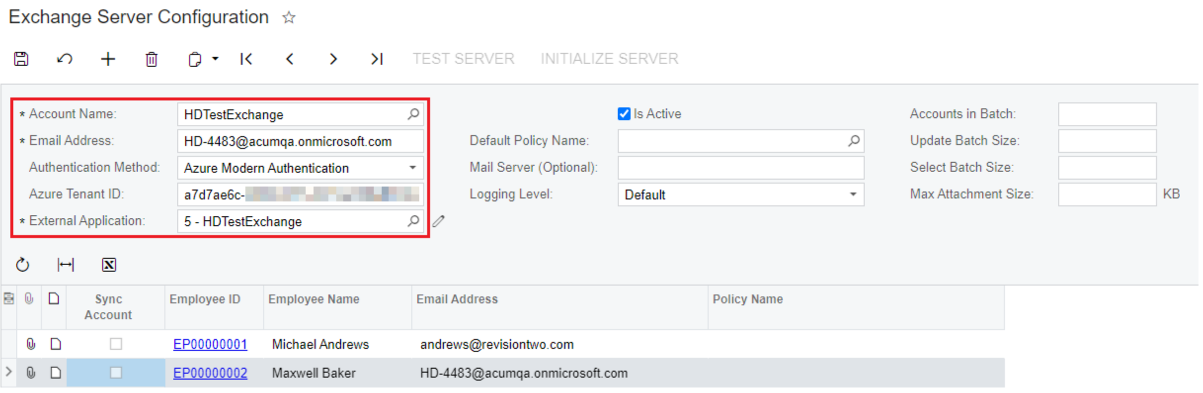
```json
{
    "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
    "resourceAccess": [
        {
            "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
            "type": "Role"
        }
    ]
}
```

3. Select **Save**.
4. Select **API permissions** under **Manage**. Confirm that the **full_access_as_app** permission is listed.
5. Select **Grant admin consent for org** and accept the consent dialog.

Step 5: On the **Exchange Server Configuration (SM204015)** form, do the following:

1. In the Account Name box, specify the account name.
2. In the **Email Address** box, specify the email address.
3. In the **Authentication Method** drop down, select the *Azure Modern Authentication or OAth2* option.
4. In the **Azure Tenant ID** box, specify the *Directory (tenant) ID* value from **Step 1**.
5. In the **External Application** box, select the external application created in **Step 3**.
6. Save your changes.

The example is shown in the following screenshot.



Exchange Server Configuration ☆

* Account Name:	HDTestExchange		☑ Is Active	Accounts in Batch:	
* Email Address:	HD-4483@acumqa.onmicrosoft.com	Default Policy Name:		Update Batch Size:	
Authentication Method:	Azure Modern Authentication	Mail Server (Optional):		Select Batch Size:	
Azure Tenant ID:	a7d7ae6c-[redacted]	Logging Level:	Default	Max Attachment Size:	KB
* External Application:	5 - HDTestExchange				

Sync Account	Employee ID	Employee Name	Email Address	Policy Name
□	EP00000001	Michael Andrews	andrews@revisiontwo.com	
□	EP00000002	Maxwell Baker	HD-4483@acumqa.onmicrosoft.com	

For more info on setting up the Exchange Integration, refer to the **Configuration Tasks** section of [Integration with Exchange Server](#) help topic.

Step 6: Click the **Test Server** button to test the account settings. The green check box on the form toolbar shows that the connection is set up.

Results

The Exchange Integration is set up using the Modern Authentication (OAuth 2.0).

C. Troubleshooting Guide:

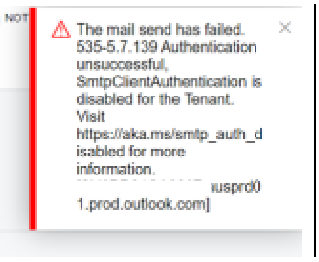
Reminders:

- If emails are setup in MYOB as both standard and exchange, 2 app registrations need to be created in Microsoft Azure
- If there are multiple primary emails in MYOB Advanced Exchange or Standard, there should be multiple External Application records .

Errors & Resolution

a. Errors on system email

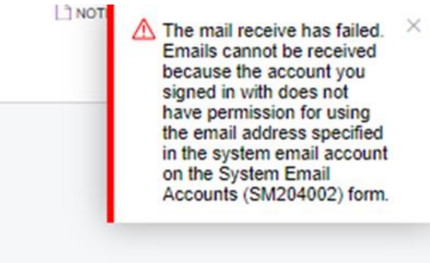
1. **The mail send has failed. 535-5.7.139 Authentication unsuccessful, SmtpClientAuthentication is disabled for the Tenant. Visit https://aka.ms/smtp_auth_disabled for more information. [SY5XXXXXXXXXX.ausprd01.prod.outlook.com]**



The mail send has failed. 535-5.7.139 Authentication unsuccessful, SmtpClientAuthentication is disabled for the Tenant. Visit https://aka.ms/smtp_auth_disabled for more information.
usprd01.prod.outlook.com]

- Resolution – Sign in on the Account and Test

2. **The mail receive has failed. Emails cannot be received because the account you signed in with does not have permission for using the email address specified in the system email account on the System Email Accounts (SM2040002) form.**

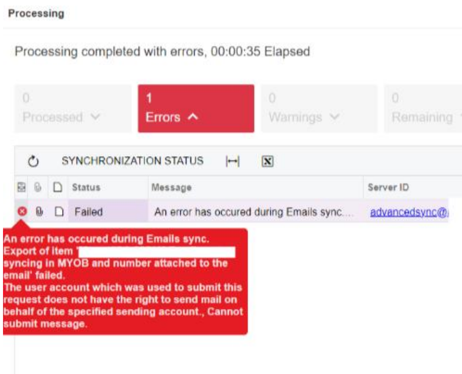


The mail receive has failed. Emails cannot be received because the account you signed in with does not have permission for using the email address specified in the system email account on the System Email Accounts (SM204002) form.

- **Resolution** – check if the following delegated permissions are available for Microsoft Graph- offline_access, IMAP.AccessAsUser.All and SMTP.Send

b. Exchange Server Configuration Errors

A. An error occurred during a simple test operation. Please check your email address, login, and password. (The specified object was not found in the store., Default folder Inbox not found.)



Processing

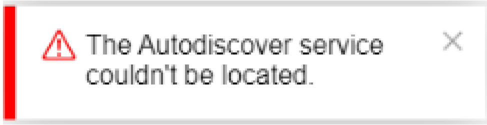
Processing completed with errors, 00:00:35 Elapsed

Status	Message	Server ID
Failed	An error has occured during Emails sync....	advancedsync@

An error has occured during Emails sync.
Export of item '[redacted]
syncing in MYOB and number attached to the email' failed.
The user account which was used to submit this request does not have the right to send mail on behalf of the specified sending account., Cannot submit message.

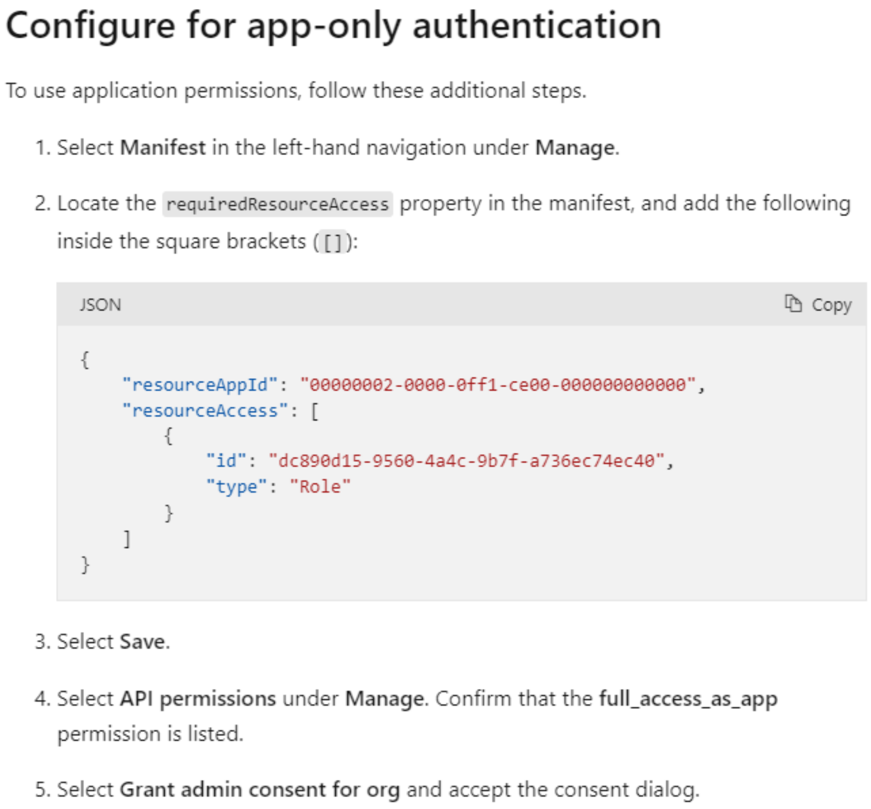
- **Resolution -** Check delegations on the email. If the email has mailbox delegated permissions to the primary email.
  - Give the email administrator full user rights to all user folders that use MYOB Advanced – Delegate access gives MYOB the ability to behave as the user and sync emails, tasks, contacts and appointments.

B. Error: The Autodiscover service couldn't be located.



The Autodiscover service couldn't be located.

- **Resolution:** Check the Manifest. The manifest should only have the details on the Json below. The api permission should only have the full_access_as_app and has granted Admin permission.



Configure for app-only authentication

To use application permissions, follow these additional steps.

1. Select **Manifest** in the left-hand navigation under **Manage**.
2. Locate the `requiredResourceAccess` property in the manifest, and add the following inside the square brackets (`[]`):

```json
{
    "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
    "resourceAccess": [
        {
            "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
            "type": "Role"
        }
    ]
}
```

3. Select **Save**.
4. Select **API permissions** under **Manage**. Confirm that the **full_access_as_app** permission is listed.
5. Select **Grant admin consent for org** and accept the consent dialog.