The page features two prominent diagonal stripes. A light blue stripe runs from the top-left corner towards the bottom-right, and a darker blue stripe runs from the bottom-left corner towards the top-right, intersecting the first stripe.

Deltek

Deltek WorkBook

Reconfiguring WorkBook to Use
Microsoft Exchange OAuth

May 30, 2024

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This publication contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or translated into another language, without the prior written consent of Deltek, Inc.

This edition published May 2024.

© Deltek, Inc.

Deltek's software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties.

All trademarks are the property of their respective owners.

Contents

Introduction.....	1
Set Up the Voucher Hot IMAP Agent.....	1
Configuration Required in your Azure Portal.....	2
Configuration Required in WorkBook.....	6
Set Up Microsoft 365 OAuth 2.0 Integration	8
Configure WorkBook	16
Troubleshooting.....	20

Introduction

Microsoft Exchange Online has deprecated Basic Authentication for multiple protocols and removed it on October 13, 2020. Basic Authentication is superseded by Modern Authentication (based on OAuth 2.0). As a result, WorkBook users may need to change the configuration of their IMAP agents and Calendar synchronization if they connect Exchange Online.

Who is affected?

- Customers who use the Voucher hot IMAP agent (Agent Type 114) and link that agent to a Microsoft Exchange IMAP server address.
- Customers who use the Calendar synchronization functionality and synchronize with a Microsoft Exchange calendar.

If you use these functions to link with products other than Microsoft Exchange, no reconfiguration is required.

Note: Some of the tasks that this document describes must be performed by a user who has Admin access to the Azure Active Directory (AD), and who may not be the WorkBook System Administrator.

Set Up the Voucher Hot IMAP Agent

The workflow for reconfiguring an IMAP agent involves the following tasks:

In Azure AD:

1. Register an application.
2. Add a client secret.
3. Grant admin consent.

In WorkBook:

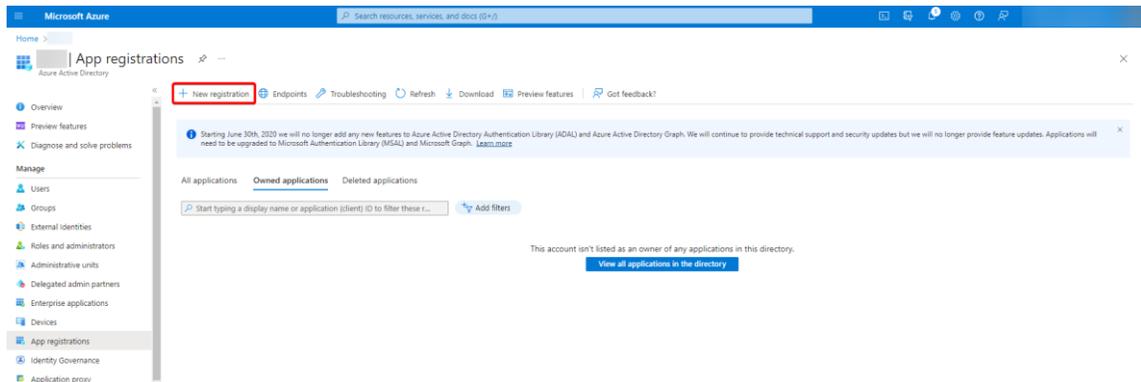
- Create a voucher hot Azure agent (Agent Type 170).

Configuration Required in your Azure Portal

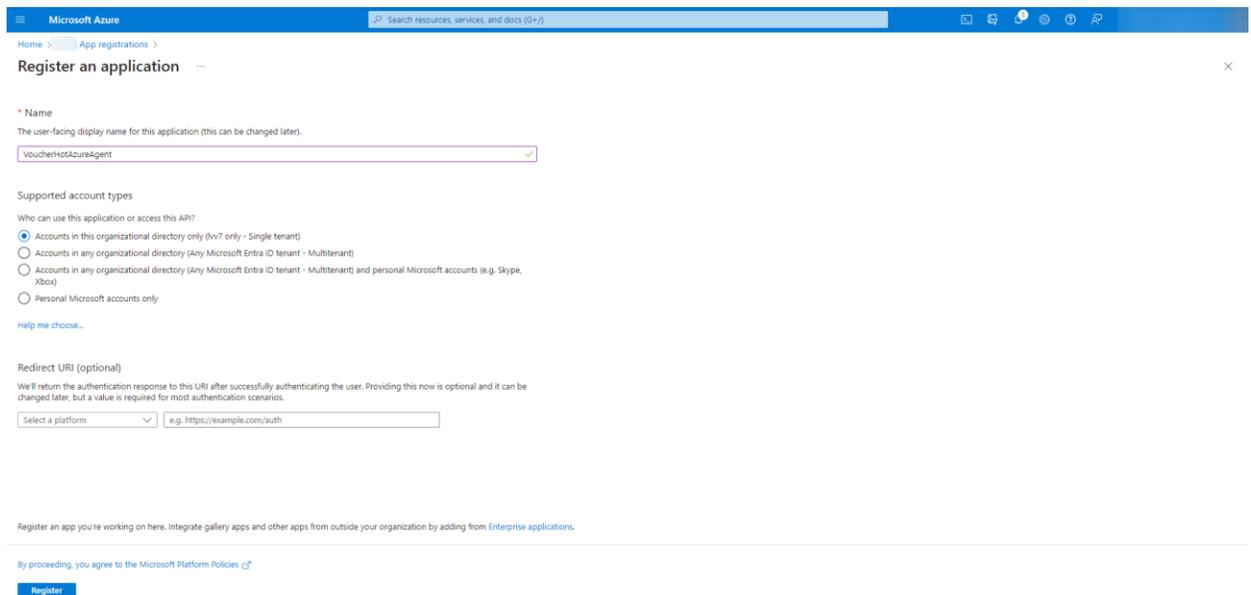
Attention: These steps must be performed by a user who has Admin access to the Azure Active Directory (AD).

To register a new application in Azure:

1. Log in to <https://portal.azure.com/>
2. Navigate to **Azure Active Directory » Manage » App registrations**.



3. Click **Register an application**. The following window is displayed.



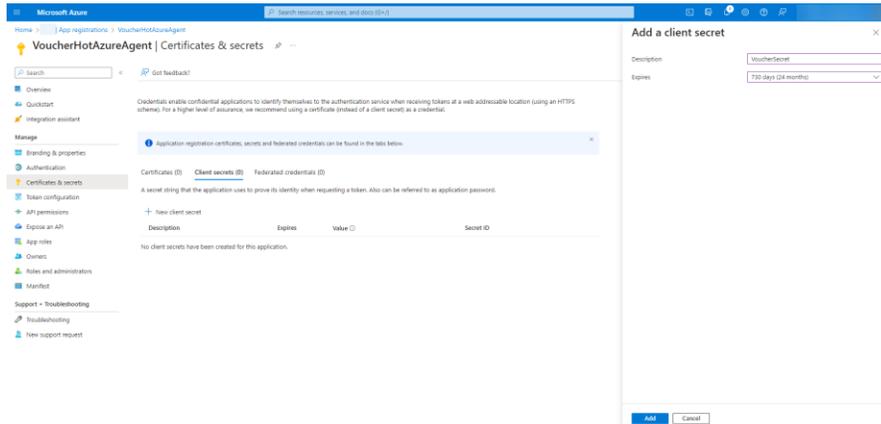
4. Enter a name for the application in the **Name** field. This is a free text field, but you should enter a meaningful name, particularly if you intend to use multiple hot Azure agents.

Supported account type defaults appropriately, based on your Azure setup. Do not change the default value.

5. Leave the **Redirect URI** field blank.
6. Click **Register**.

Set Up the Voucher Hot IMAP Agent

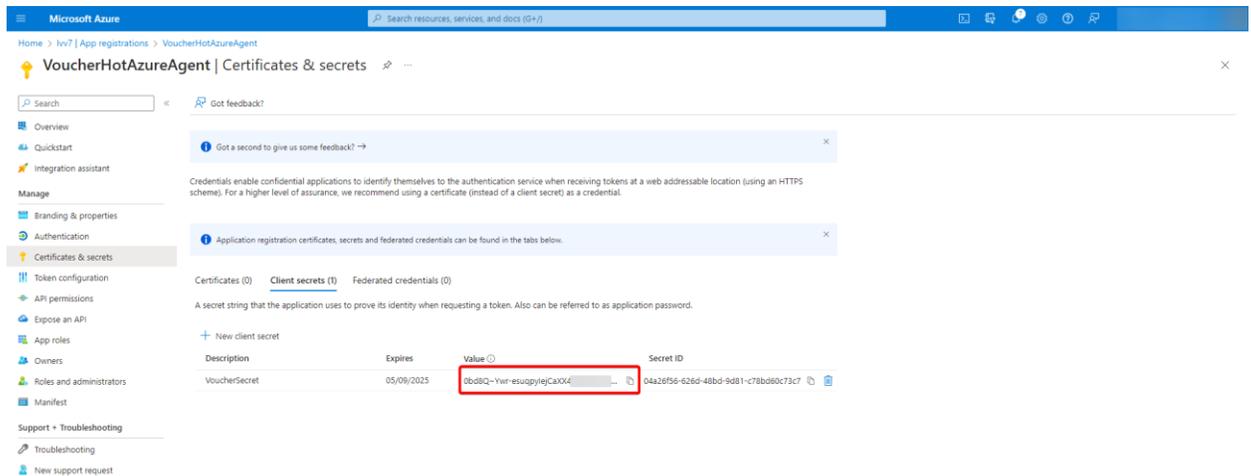
- Navigate to **Manage » Certificates & secrets**. The **Add a client secret** dialog is displayed.



- Add a client secret and copy the value, because this is the only time that you can see it.
- Enter the description and indicate whether you want the secret to expire.

Having a secret expire instead of being retained indefinitely means that you must generate a new secret. You may also want to delete the secret and create another one even more frequently than once a year.

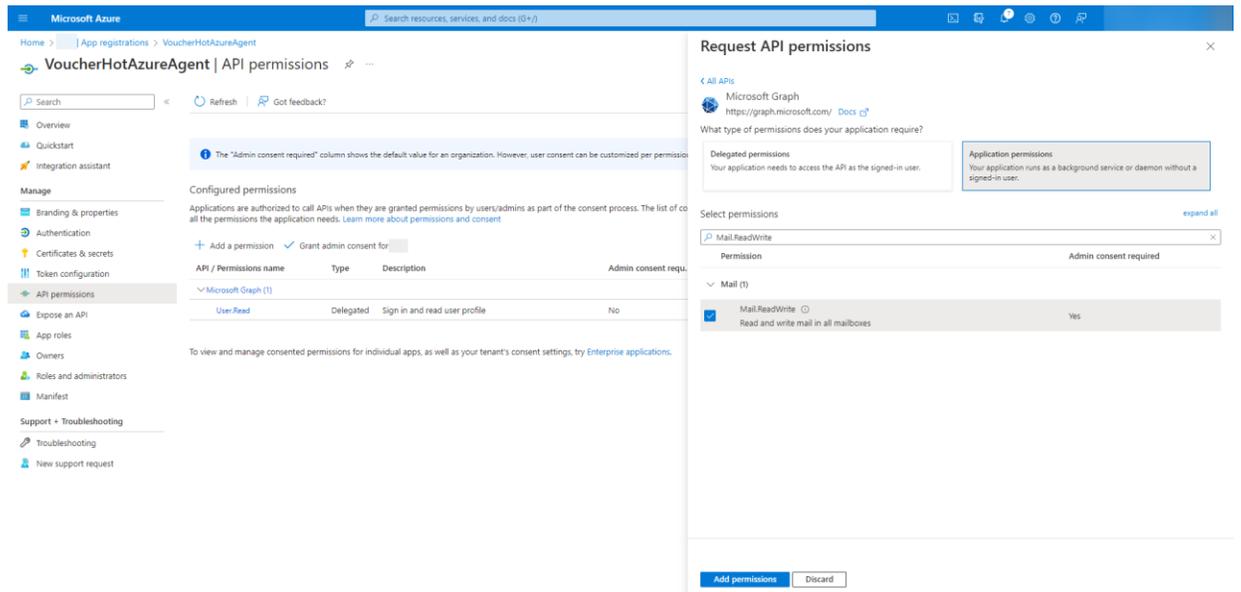
Make sure that you do not leave the client secret in a place where others can access it, because this secret is used for authentication purposes. If you left the page without copying down the value, or you managed to lose it, you must delete the secret and create another one.



- Navigate to **Manage » API permissions**. The **Configured permissions** pane is displayed.

Set Up the Voucher Hot IMAP Agent

11. Click **Add a permission**. The **Request API permissions** pane is displayed.

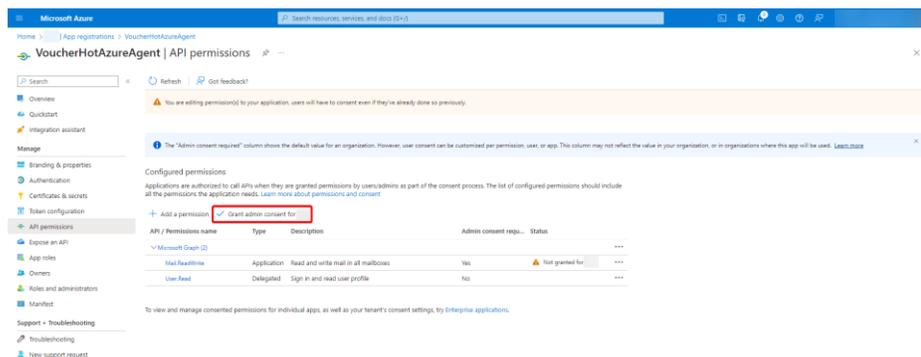


12. Add a permission for **Mail.ReadWrite**:

- Select **Application permission**; otherwise, the Mail.ReadWrite permission is not displayed.
- Search for the permission **Mail.ReadWrite** and select its checkbox.

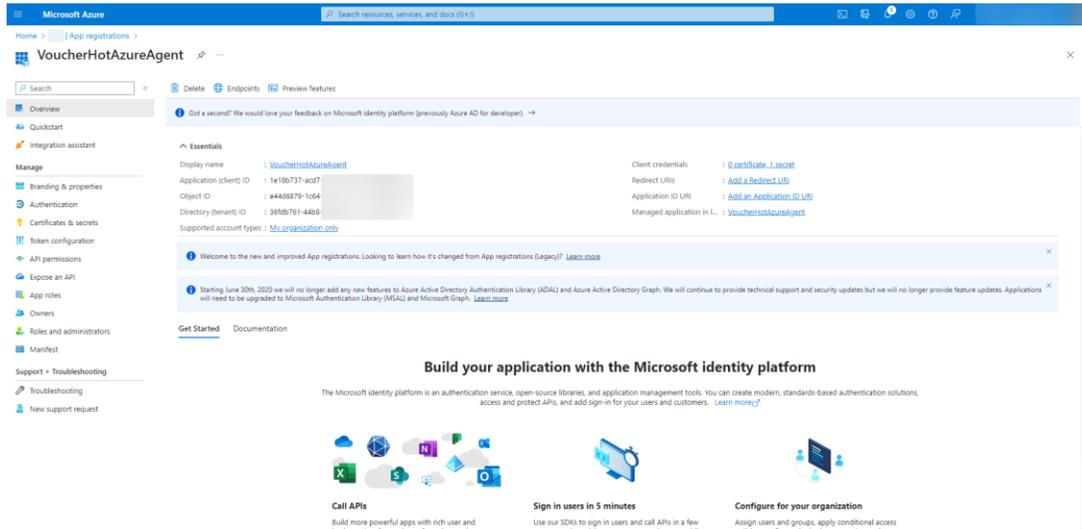
13. Click **Add permissions** at the bottom of the **Request API permissions** pane.

This takes you to the **API permissions Configured permissions** pane.



14. Click **Grant admin consent**. This button name varies because it includes your specific Azure service name.

15. Navigate to **Overview**.



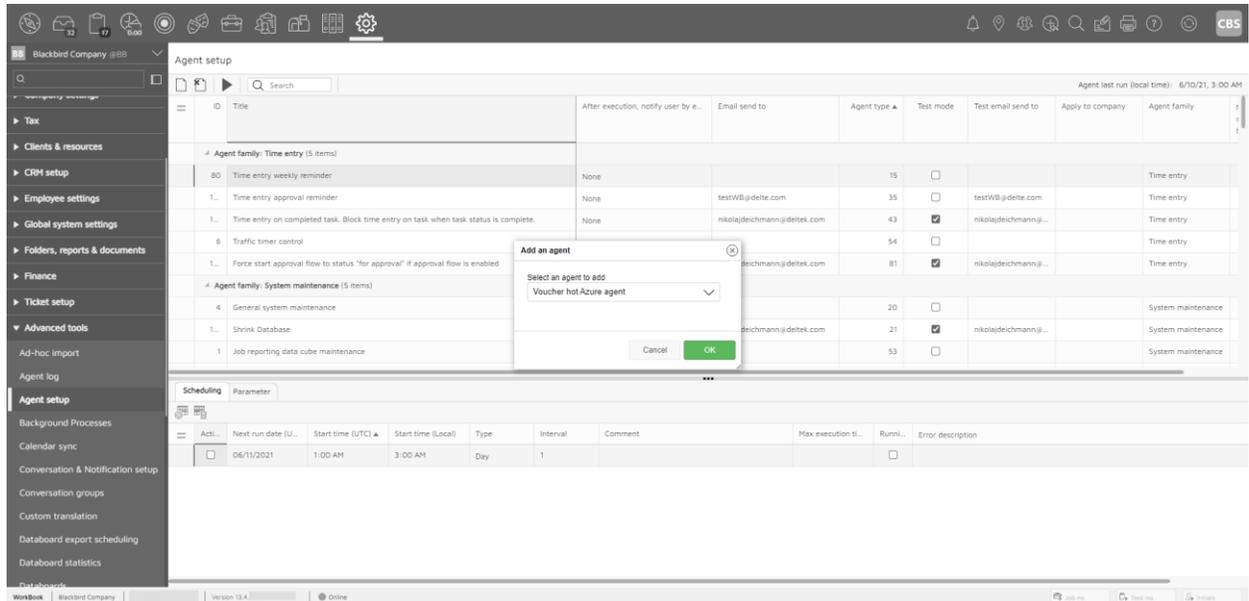
Tip: Write down the values of the **Application (client) ID** and **Directory (tenant) ID** indicated for the Application that you just registered. You need to know these values to perform the configuration in WorkBook that is described in the next procedure.

Configuration Required in WorkBook

These steps must be performed by either a WorkBook System Administrator or an Advanced User who has access to Settings » Agent Setup.

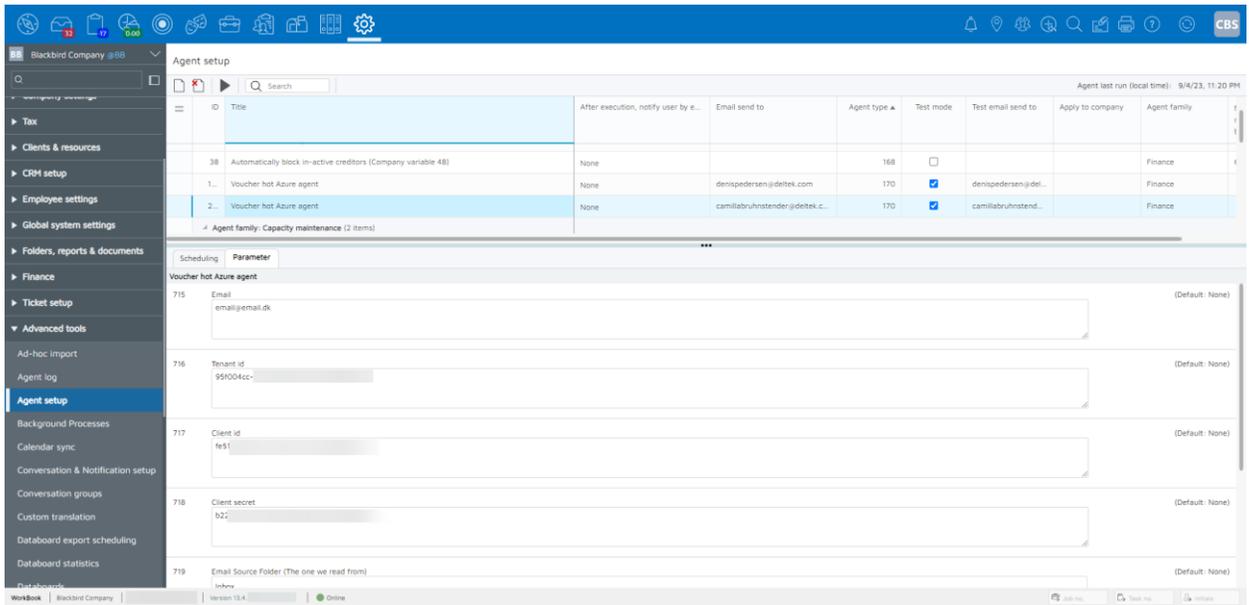
To set up the voucher hot Azure agent:

1. Go to WorkBook and navigate to **Settings » Advanced Tools » Agent Setup**.
2. Click  **Add Agent**. The **Add an Agent** dialog is displayed.



3. Select **Voucher hot Azure agent** from the **Select an agent to add** drop-down list.
4. Enter the parameters for the agent:
 - **Email** – The email address that is to be linked to
 - **Tenant ID** – To be obtained from the application in the Azure portal
 - **Client ID** – To be obtained from the application in the Azure portal
 - **Client secret** – To be obtained from the application in the Azure portal

Set Up the Voucher Hot IMAP Agent



After you have entered these parameters, the agent definition is complete. When you schedule it, the agent operates as a hot IMAP agent, using Microsoft OAuth.

Set Up Microsoft 365 OAuth 2.0 Integration

Register your Application in Azure Portal

To register your application in Azure Portal:

1. Enter the Redirect URI.

The integration works for multi-tenant as well as single-tenant applications.

Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only only - Single tenant

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Attention: Deltek recommends that you create one application registration instead of several.

Add Permissions to your Application

To add permissions to your application in the API permissions / Add a permission wizard:

1. For all: User.Read, offline_access as type delegated

Set Up Microsoft 365 OAuth 2.0 Integration

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](#)

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>▼ OpenId permissions (1)</p>	
<input checked="" type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No

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](#)

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>▼ OpenId permissions (1)</p>	
<input checked="" type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No
<input type="checkbox"/> email ⓘ View users' email addresses	No
<input type="checkbox"/> openid ⓘ Sign users in	No
<input type="checkbox"/> profile ⓘ View users' basic profile	No

2. For mail import:
 - Imap.AccessAsApp as type application
 1. In the Azure portal, choose the **API Permissions blade** in your Azure AD application's management view.
 2. Select **Add permission**.
 3. Select the **APIs my organization uses** tab and search for **Office 365 Exchange Online**.

Request API permissions ×

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

Office 365 Exchange Online	Application (client) ID
Office 365 Exchange Online	[REDACTED]

4. Click **Application permissions**.
5. For IMAP access, choose the **IMAP.AccessAsApp** permission.

6. Choose **Mail.ReadWrite**.

Request API permissions ×

[← All APIs](#)

Office 365 Exchange Online
<https://outlook.office.com>

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

Permission	Admin consent required
> Other permissions	
> Calendars	
> Contacts	
> Exchange	
IMAP (1)	
<input checked="" type="checkbox"/> IMAP.AccessAsApp ⓘ IMAP.AccessAsApp	Yes
> Mailbox	
> MailboxSettings	
Mail (1)	
<input type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes

Set Up Microsoft 365 OAuth 2.0 Integration

7. After you choose the type of permission, select **Add permissions**.
 - Mail.ReadWrite as type application under **Microsoft Graph**

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](#)

Permission	Admin consent required
> MailboxSettings	
▼ Mail (1)	
<input type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
<input type="checkbox"/> Mail.Send ⓘ Send mail as any user	Yes

3. For mail send:

- Mail.Send as type application
- Mail.ReadWrite as type application

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.

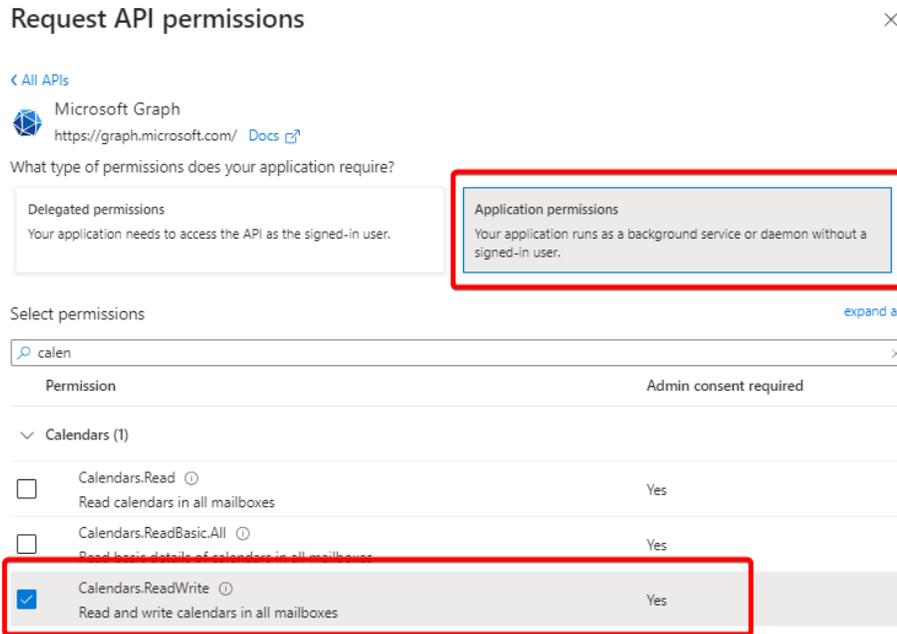
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
> MailboxSettings	
▼ Mail (2)	
<input type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as any user	Yes

Set Up Microsoft 365 OAuth 2.0 Integration

- 4. For calendar:
 - Calendars.ReadWrite as type application



The following example shows the resulting permissions setup for calendar, mail import, and mail send:

Configured permissions

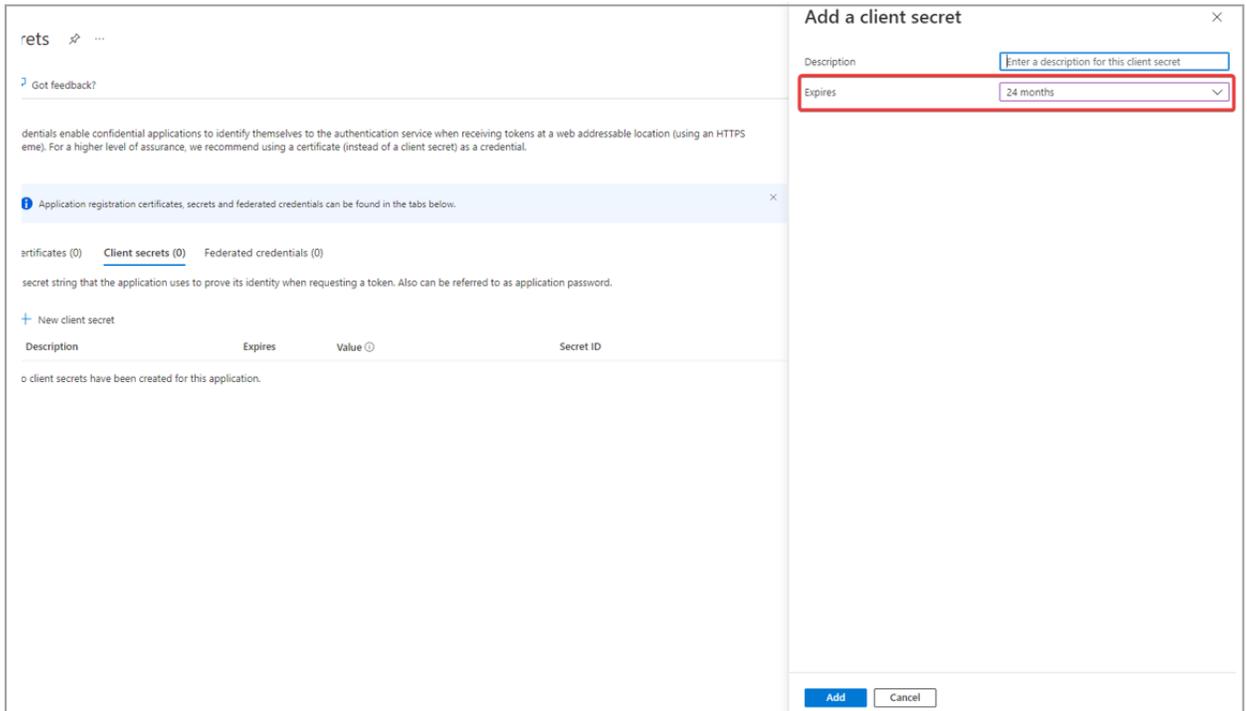
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permission all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for DeltekDemo.com

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (5)				
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	✓ Granted for
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
▼ Office 365 Exchange Online (2)				
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	✓ Granted for
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for

Note: You must grant all consents for permissions to work correctly.

5. Click the **New Client Secret** button in the **Certificates and Secrets** panel to create an application secret.



6. Select a value for the **Expires** field. The integration will work until this time period elapses.

Tip: Be sure to refresh the secret **before** it expires.

Configure OAuth 2.0 for Office 365 Mailing

To configure OAuth 2.0 for Office 365 mailing:

Enable IMAP for your organization and mailbox:

1. Navigate to the Microsoft 365 admin portal at <https://admin.microsoft.com/> and log in as Administrator.
2. Go to **Settings » Org Settings**.
3. Select **Modern authentication** and select **Turn on modern authentication for OAuth flows**.

Enable Use of PowerShell

To use Windows PowerShell on your computer to register service principals in Exchange:

1. Set the execution policy:


```
Set-ExecutionPolicy RemoteSigned
```
2. Install the ExchangeOnlineManagement module:


```
Install-Module -Name ExchangeOnlineManagement
Import-Module ExchangeOnlineManagement
```

Set Up Microsoft 365 OAuth 2.0 Integration

3. Connect, and then log in as Administrator. (You are prompted for the password.)

```
Connect-ExchangeOnline -UserPrincipalName your-admin-account@your-domain.onmicrosoft.com
```

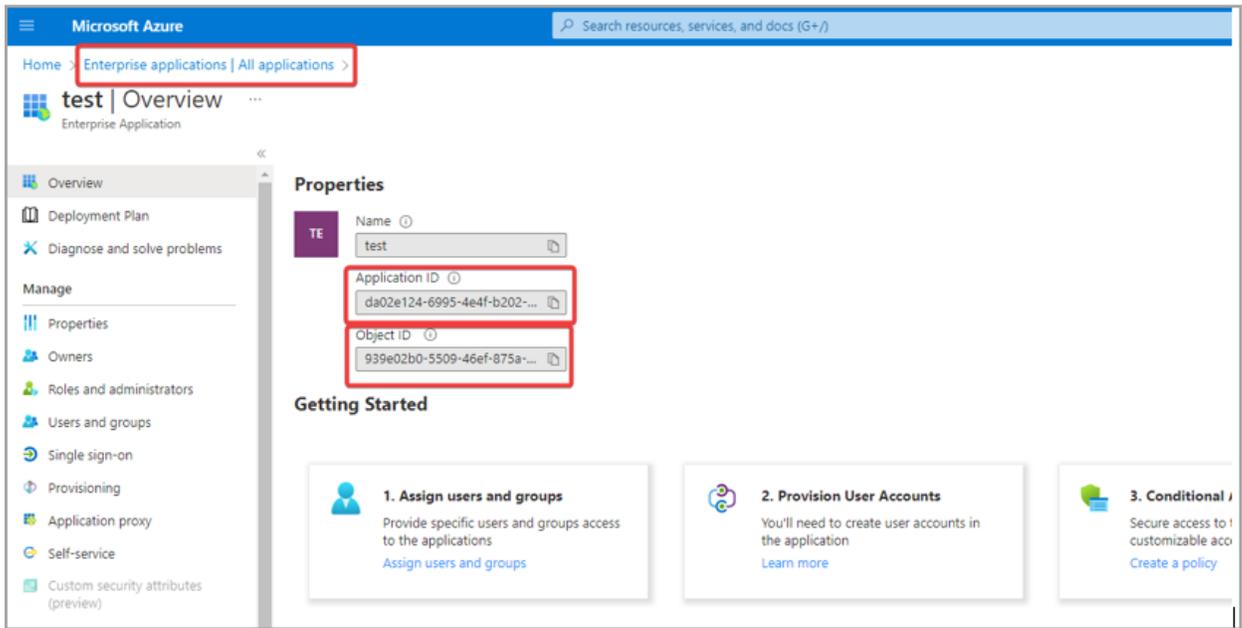
4. For Exchange running in hybrid mode, log in using the following code:

```
$lc = Get-Credential
Connect-ExchangeOnline -Credential $lc
```

5. Create the service principal:

```
New-ServicePrincipal -AppId <APPLICATION_ID>
-ServiceId <OBJECT_ID> [-Organization <ORGANIZATION_ID>]
```

Ensure that you use the Object ID from the Enterprise Application:



6. Add permissions to a specific mailbox:

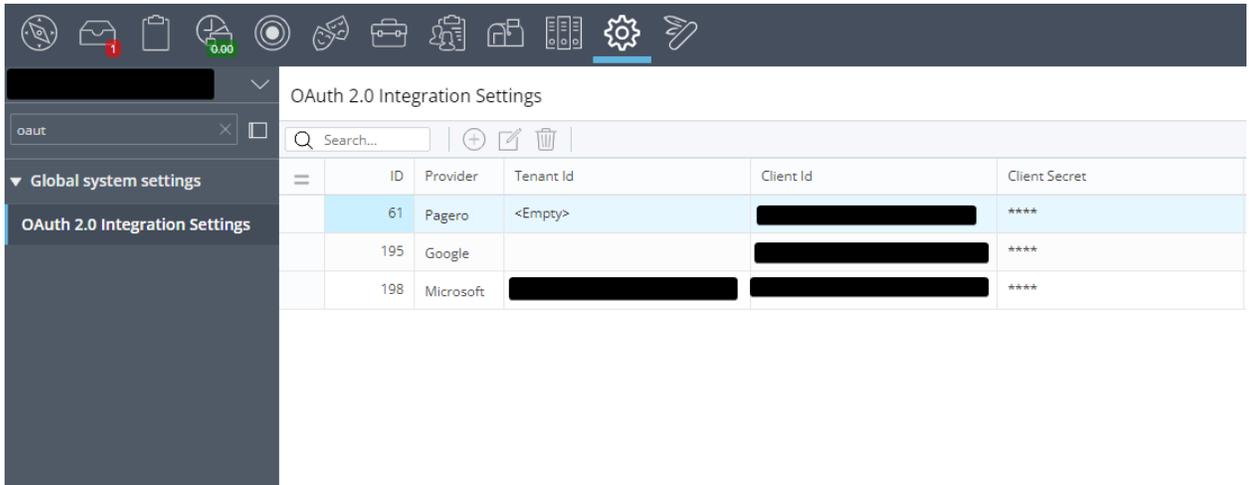
```
Add-MailboxPermission
-Identity "<USER@your-domain.onmicrosoft.com>"
-User <OBJECT_ID>
-AccessRights FullAccess
```

You must use Add-MailboxPermission for every shared mailbox to which you require access.

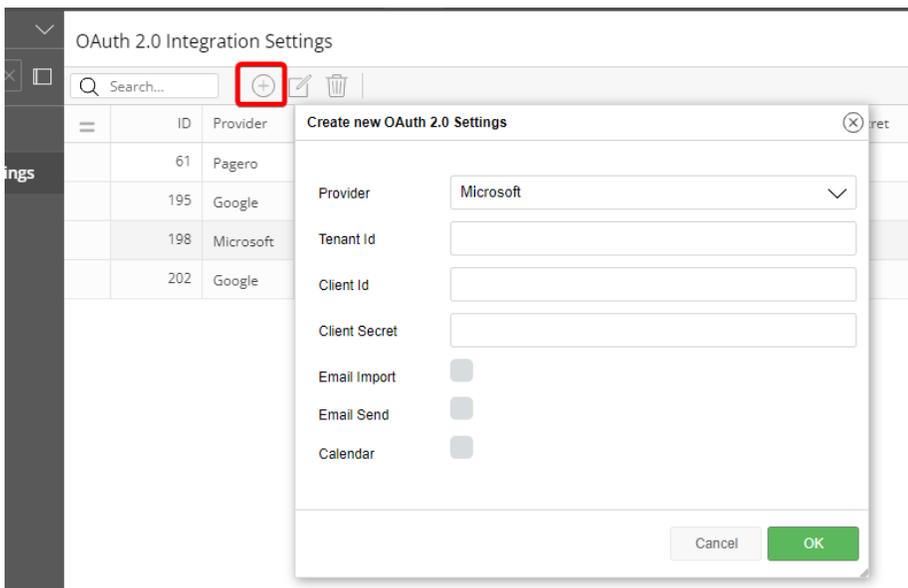
Configure WorkBook

To configure WorkBook:

1. Navigate to **Settings » Global System Settings » OAuth2 Integration Settings**.



2. If you do not have one, create the setting.

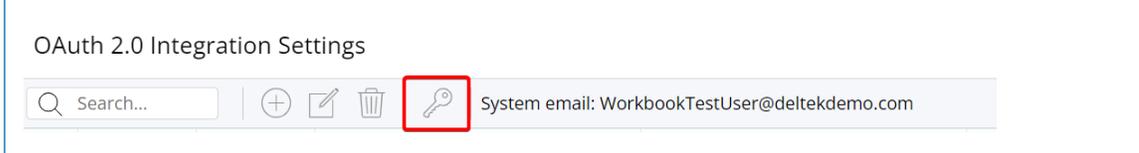


Set Up Microsoft 365 OAuth 2.0 Integration

3. Select the Microsoft provider; enter the tenant ID, client ID, and client secret. Check the scopes that you want to set up.

Note: If you select the Email Send you are asked to log in right after you click OK. You can have only one email set up that you can send emails with. If the login fails you can log in again by clicking the  key button on the grid toolbar. This button appears when you select a row that includes Email Send scope.

The actual email address that is used for sending email is displayed next to the key button.

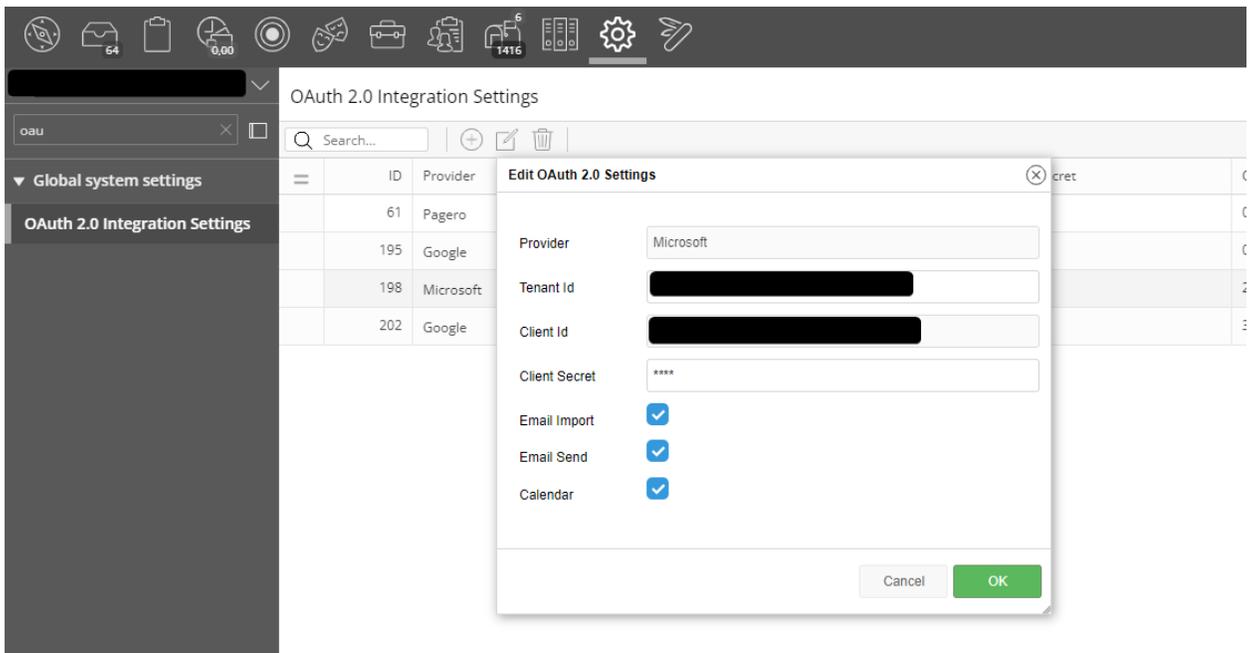


The following are the settings constraints:

- Client ID must be unique across all settings. You cannot edit it after you have created the settings.
- Email Import – You can have only one setting with Email Import scope per list.
- Email Send – You can have only one setting with Email Send scope in the list.
- Calendar – You can have only one setting per provider in the list.

If you want to create a setting when a setting with the same scope already exists in the list, and one of the constraints is met, the existing setting is disabled.

If you have an existing setting, and you want to update the client secret or add/remove scopes, you can do it by using the Edit OAuth 2.0 Settings dialog box as shown in the following example.



Additional Notes:

Email Send

WorkBook can send emails with the primary account (defined in System Variable 289) or with individual accounts (check System Variable 760). See [Configure OAuth 2.0 for Office 365 Mailing](#).

- The domain that is used in the primary account (defined in System Variable 289) as well as other domains that are used for sending emails should be verified.

Email Import

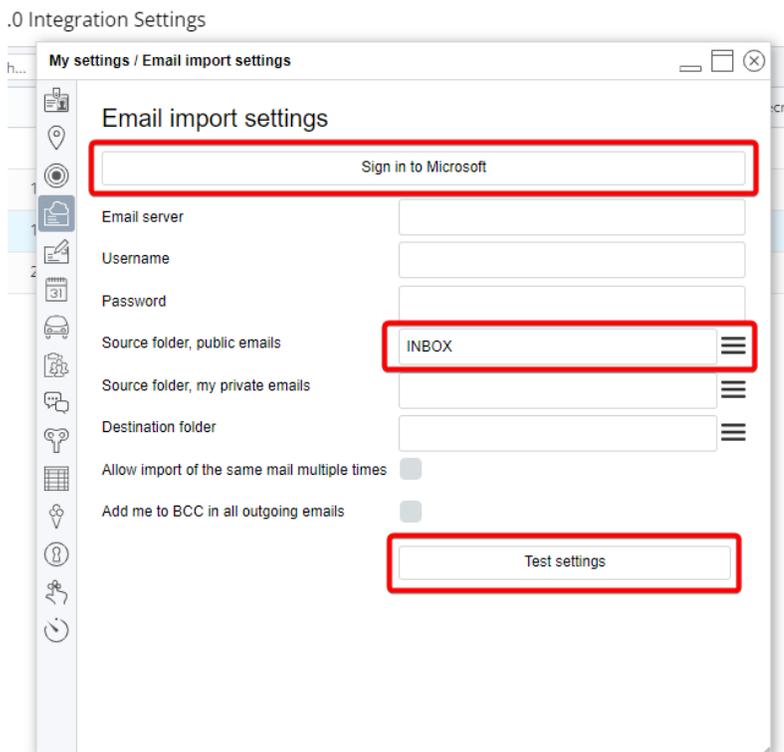
The import happens through the agents. Go to Agent Setup and take advantage of the following OAuth 2.0 agents:

- Mail Archive Agent (OAuth 2.0)
- Mail Import Agent (OAuth 2.0)
- Mail Import Public Agent (OAuth 2.0)

Test Mail Import

To test your OAuth 2.0 setup with User Settings – Email import settings:

1. Navigate to **My Settings » Email import settings** and sign in with Microsoft.
2. Select the source folder and test settings. If it is successful, the configuration for this user works correctly.



3. Select the folders that are to be used as Source folder public and private emails and Destination folder.

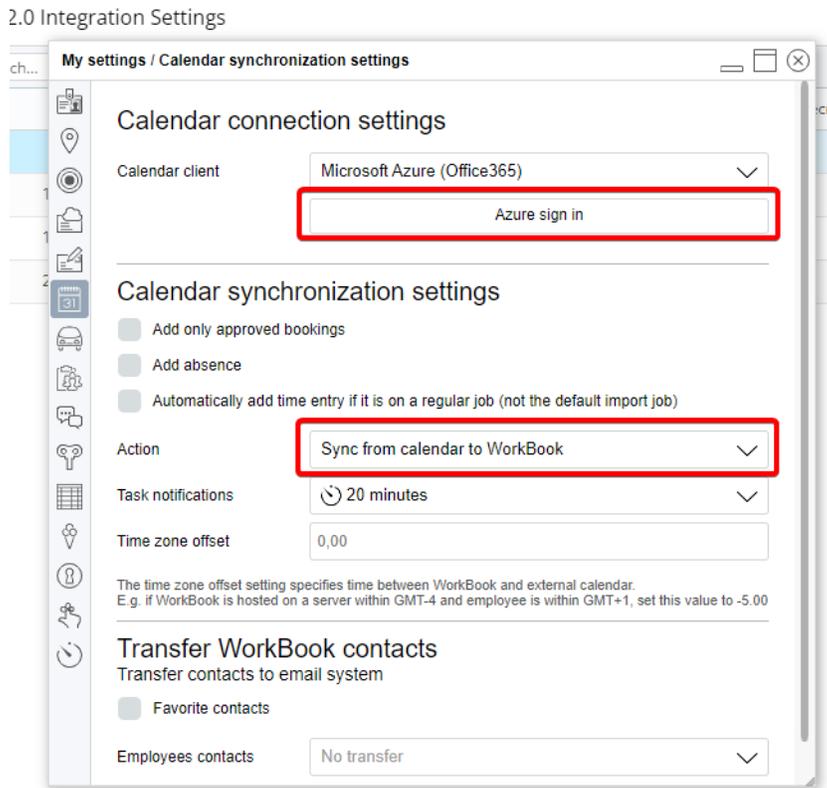
Set Up Microsoft 365 OAuth 2.0 Integration

4. Go to Agent Setup and take advantage of the following OAuth 2.0 agents:
 - Mail Archive Agent (OAuth 2.0)
 - Mail Import Agent (OAuth 2.0)
 - Mail Import Public Agent (OAuth 2.0)

Test Calendar

To test the calendar:

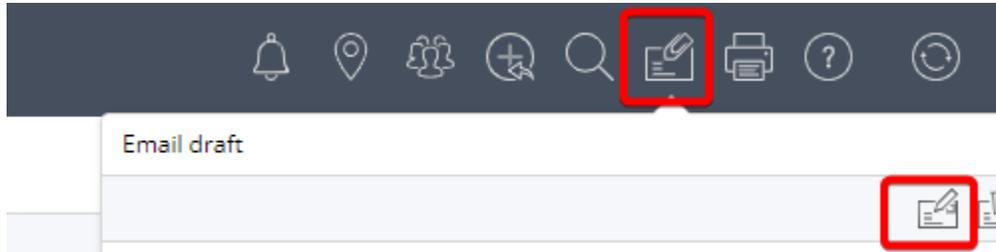
1. Navigate to **My Settings » Calendar** and sign in with Microsoft.
2. Select calendar sync options.
3. Create events that can be synced to WorkBook.
4. Run the Calendar agent and check the logs to confirm that the connection was successful.



Test Mail Send

To test sending an email:

1. Send an email using **Email Drafts » Compose New Email** on the main toolbar.



Troubleshooting

1. Check the permissions:

```
Get-ServicePrincipal
Get-MailboxPermission -Identity <email_address>
```

1. Check the **Tenant Id**, **Client Id**, and **Client Secret** fields.
2. Ensure that you took the **Objectid** from the Enterprise Application page.
3. Ensure that you added the correct permissions and granted **Admin consents**.

Depending on your security settings for your Exchange account, Administrators may need to approve users manually when they authorize access to their own Outlook.

About Deltek

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 23,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. www.deltek.com