

Time Matters and Office 365 Modern Authentication Setup

10/04/2022

Robert Gray, CIC

Legality Software/Matters in Motion, Inc.

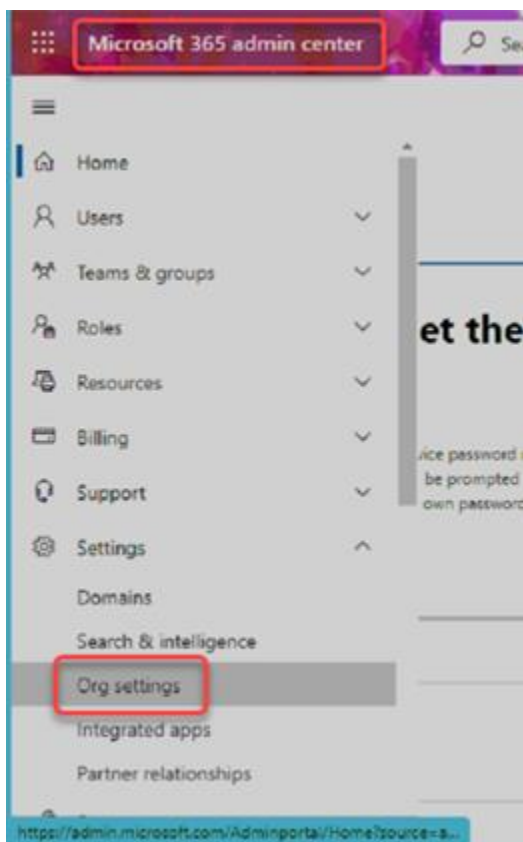
support@mattersinmotion.com

NOTICE: These instructions include details of the settings behind our research and successful testing at multiple client sites. We've made our best effort to provide accurate information here, but be aware we may have missed something. P|T developers created the TM code and are the ultimate authority on how TM accesses the 365 Hosted Exchange servers. So far, P|T has not shared those details, so we're doing our best to help the community with this document. Use your own judgement on the viability of these settings and any potential security risks. You are ultimately responsible for any issues that arise from attempting this setup. In YouTube style, this information is provided for entertainment purposes only.

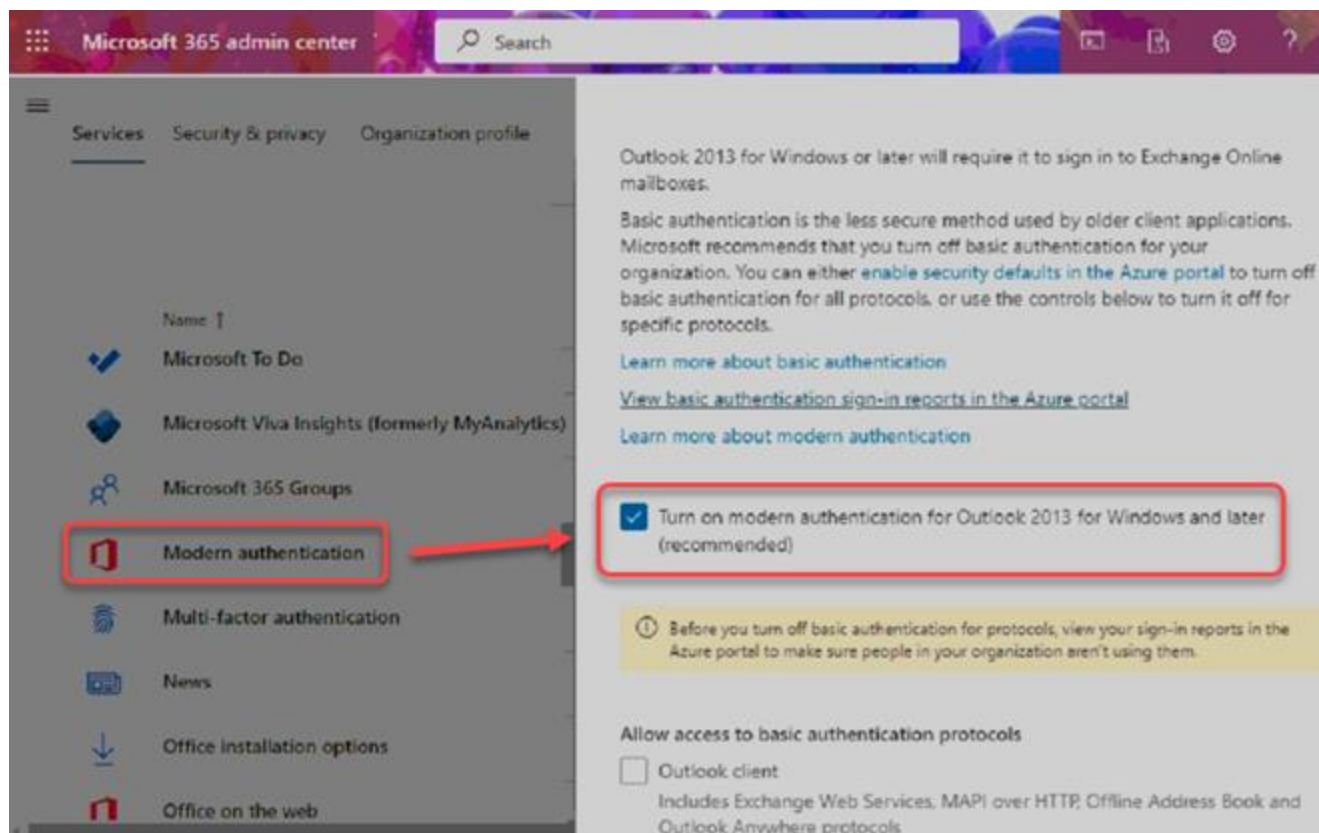
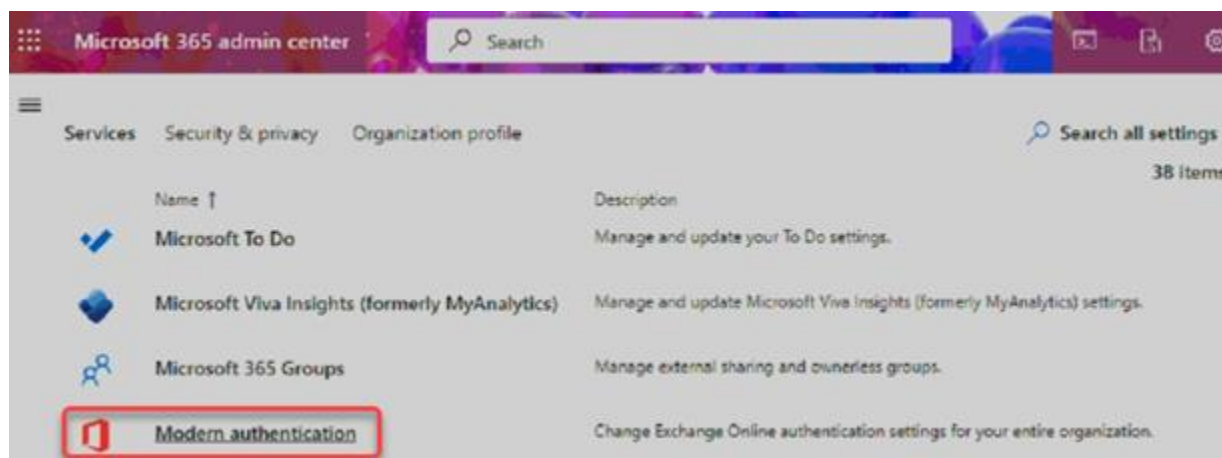
Enable 'Modern Authentication' - 365 Admin Console

<https://admin.microsoft.com/Adminportal/Home>

Log in to the "Microsoft 365 admin center" and click "Settings | Org settings" from the left menu.



Click “Modern Authentication” in the list.



NOTE: You should consider whether or not to disable these basic authentication protocol options. The risk is some users or apps might still depend on them. Here's an article to help you decide:

<https://lazyadmin.nl/office-365/modern-authentication-office-365>

Microsoft 365 admin center Search

Services Security & privacy Organization profile

Name ↓

- Microsoft Viva Insights (formerly MyAnalytics)
- Microsoft 365 Groups
- Modern authentication**
- Multi-factor authentication
- News
- Office installation options
- Office on the web

Modern authentication

Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA). When you turn on modern authentication, Outlook 2013 for Windows or later will require it to sign in to Exchange Online mailboxes.

Basic authentication is the less secure method used by older client applications. Microsoft recommends that you turn off basic authentication for your organization. You can either [enable security defaults in the Azure portal](#) to turn off basic authentication for all protocols, or use the controls below to turn it off for specific protocols.

[Learn more about basic authentication](#)

[View basic authentication sign-in reports in the Azure portal](#)

[Learn more about modern authentication](#)

☒ Turn on modern authentication for Outlook 2013 for Windows and later (recommended)

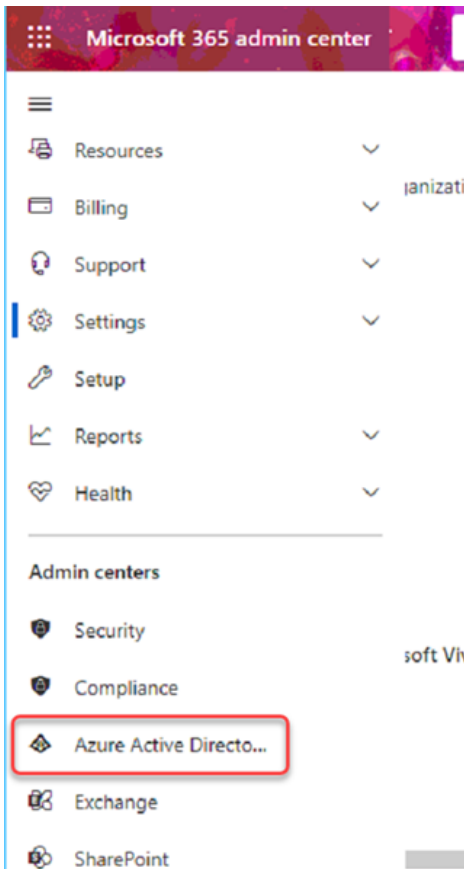
ⓘ Before you turn off basic authentication for protocols, view your sign-in reports in the Azure portal to make sure people in your organization aren't using them.

Allow access to basic authentication protocols

- ☒ Outlook client
Includes Exchange Web Services, MAPI over HTTP, Offline Address Book and Outlook Anywhere protocols
- ☒ Exchange ActiveSync (EAS)
Used by some email clients on mobile devices.
- ☒ Autodiscover
Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.
- ☐ IMAP4
Used by IMAP email clients.
- ☐ POP3
Used by POP email clients.
- ☐ Authenticated SMTP
Used by POP and IMAP clients to send email messages.
- ☒ Exchange Online PowerShell
Used to connect to Exchange Online with remote PowerShell. [Learn more](#)

Create an “Enterprise App” entry - 365 Admin Console

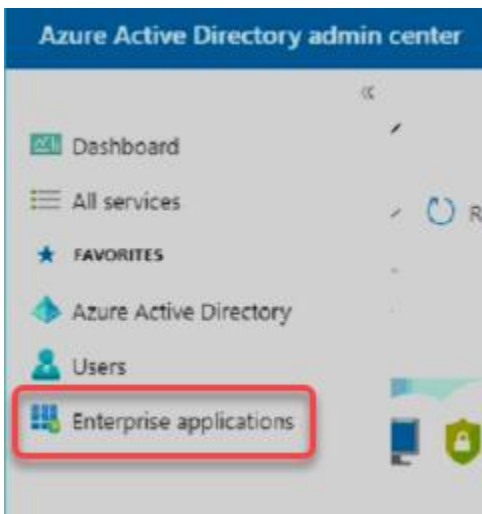
Click “Azure Active Directory” under the “Admin Centers” section of the left menu.



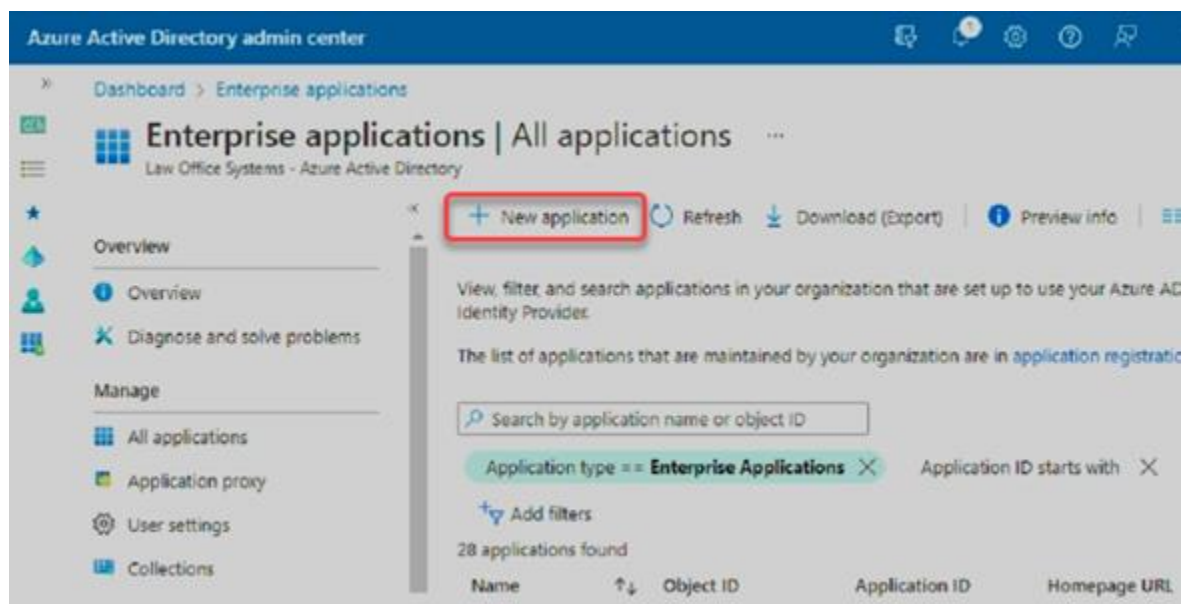
A new tab opens to the “Azure Active Directory admin center”

<https://aad.portal.azure.com>

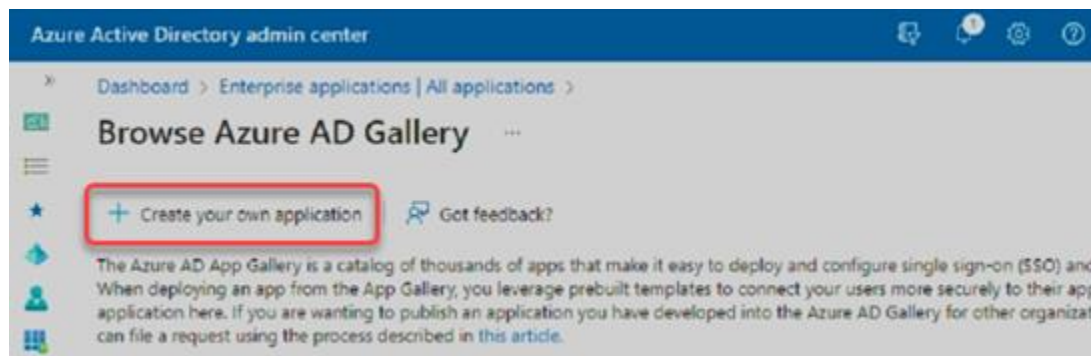
Click “Enterprise applications” in the left menu. NOTE: You may have to select “All Services” then pick “Enterprise applications” from the list on the right.



Click "+ New application"

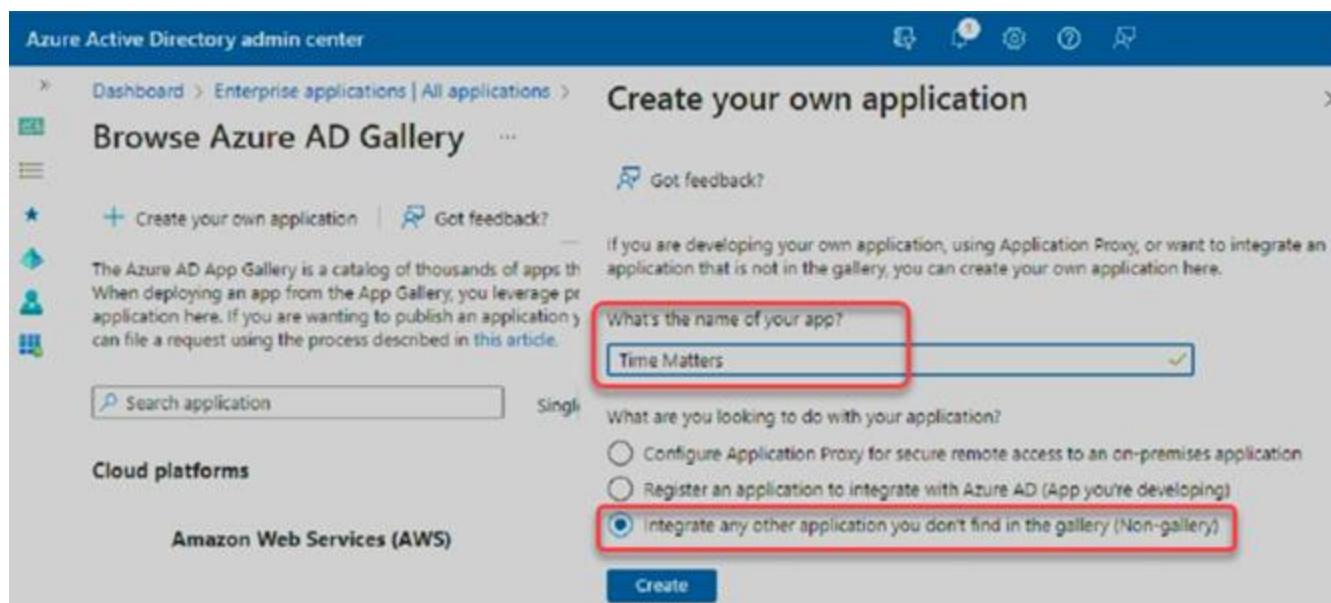


Click "+ Create our own application"



Enter whatever name you want to use. This could be "Time Matters" or "TM-Exchange Sync" or whatever you like.

Keep the default "Integrate any other..." option and click <Create>



Save the “Application ID” value for the TM Exchange Configuration Utility.

Azure Active Directory admin center

Dashboard > Enterprise applications | All applications > Browse Azure AD Gallery >

Time Matters | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning

Properties

TM

Name ⓘ Time Matters

Application ID ⓘ ffd066aa-...

Object ID ⓘ 6effa147-...

Getting Started

1. Assign users and groups

Enter in TM-Exchange Configuration Utility 'Client ID' field.

Ignore

Click “Properties” under the “Manage” section of the left menu.

Set these options as shown and click <Save>.

Azure Active Directory admin center

Dashboard > Enterprise applications | All applications > Browse Azure AD Gallery > Time Matters

Time Matters | Properties

Enterprise Application

Save Discard Delete Got feedback?


View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the application registration.

Enabled for users to sign-in? Yes No

Name * Time Matters Test ✓

Homepage URL

Logo  Select a file

User access URL <https://myapps.microsoft.com/signin/ffd066aa-2ec1-4e2d-...>

Application ID ffd066aa-...

Object ID 6effa147-...

Terms of Service Url Publisher did not provide this information

Privacy Statement Url Publisher did not provide this information

Reply URL Publisher did not provide this information

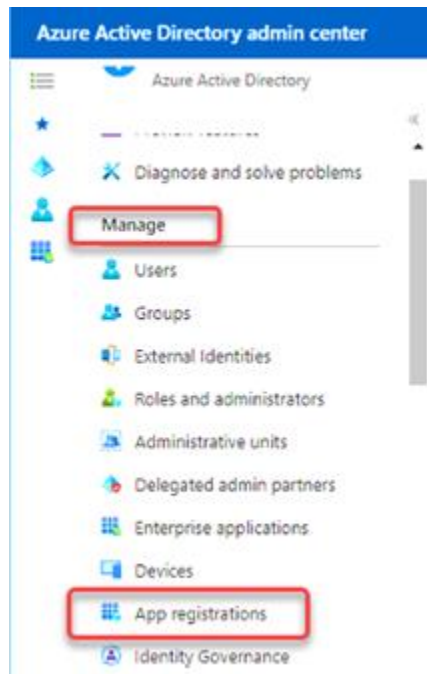
Assignment required? Yes No

Visible to users? Yes No

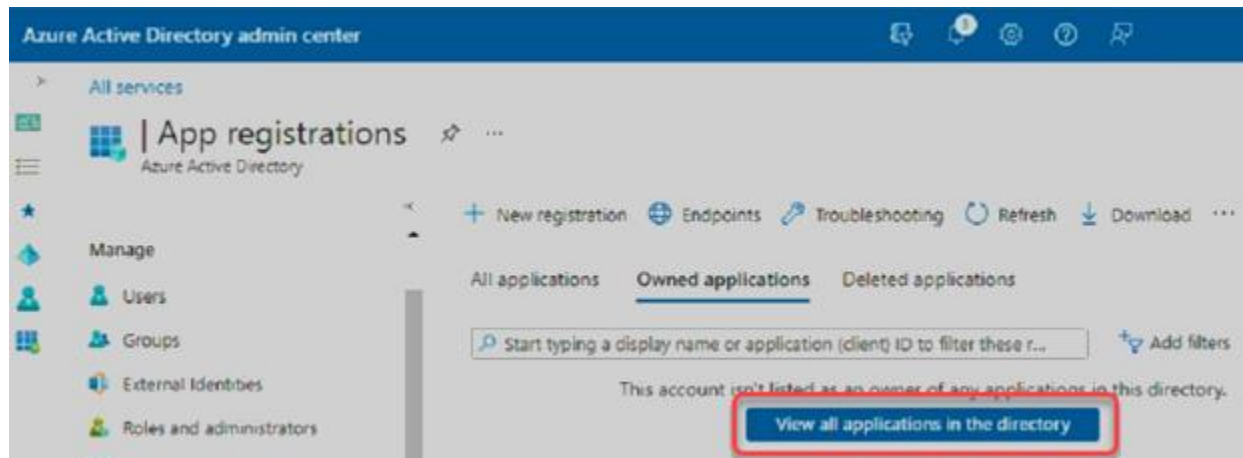
Notes

Create the “Client Secret”

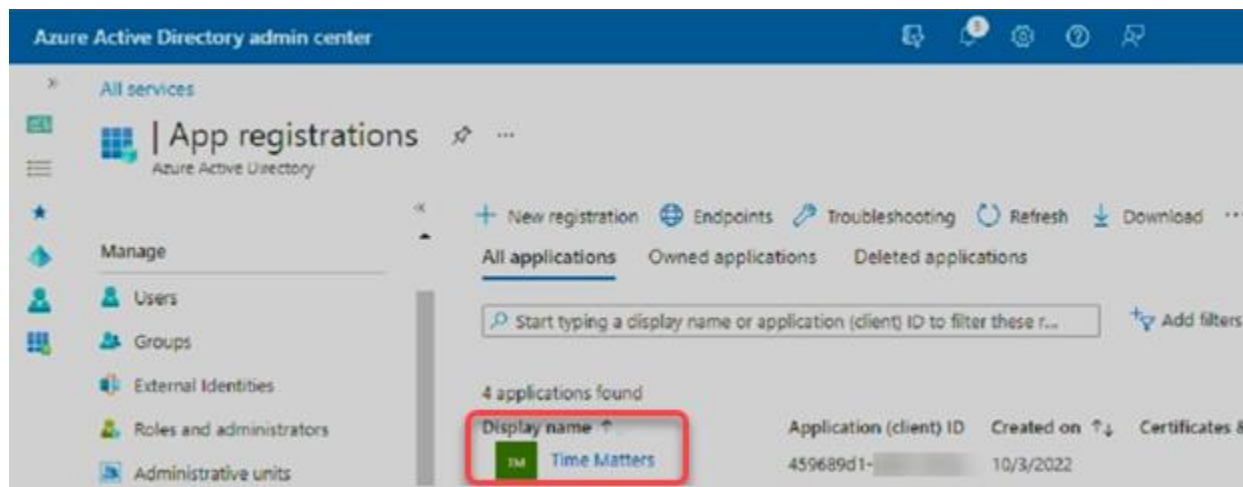
Click “Azure Active Directory” then “App registrations” under the “Manage” section of the left menu.



Click <View all applications in the directory> if your TM application entry isn’t visible.

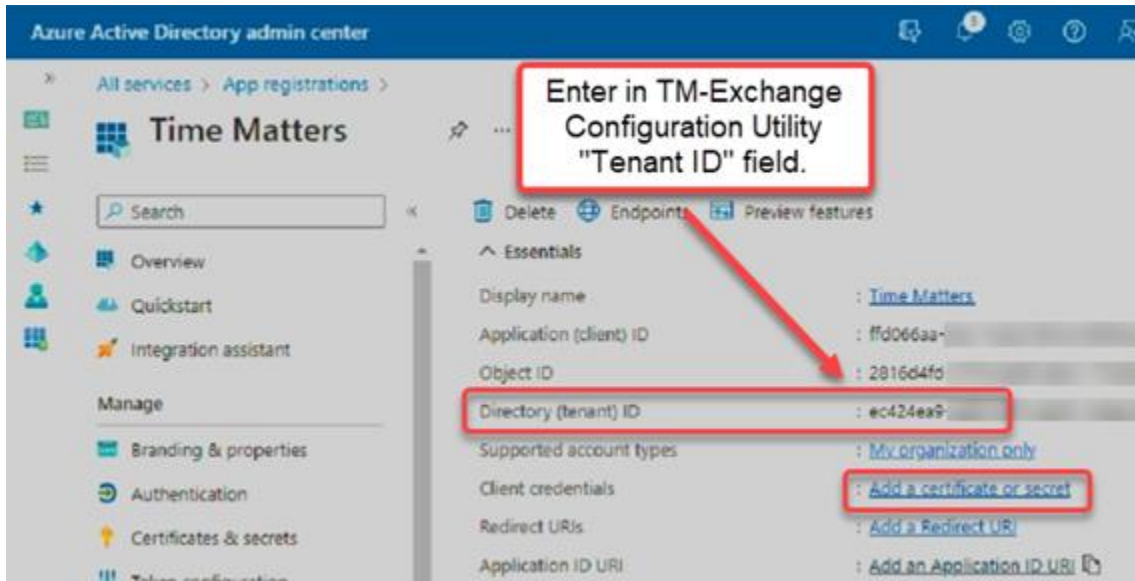


Click your TM application in the list.

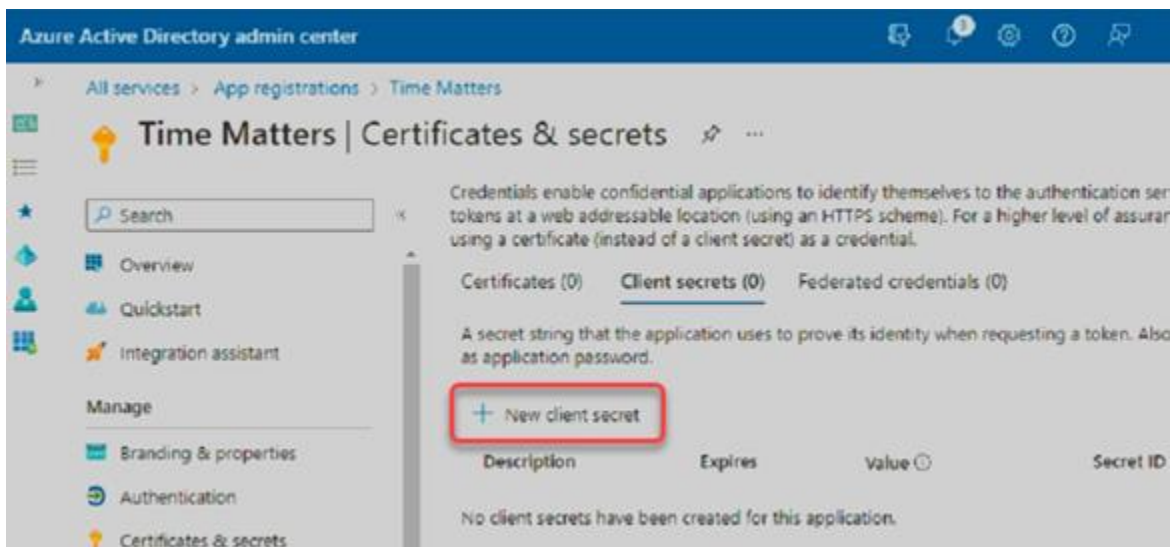


Save the “Tenant ID” value for the TM Exchange Configuration Utility.

Click the “Add a certificate or secret” link.



Click “+ New client secret”



Enter a name for your client secret and choose an active period with an expiration date.

NOTE: The “Expires” dropdown list ranges from 3 to 24 months. The “Custom” option doesn’t extend that beyond 24 months. Regardless of the period you choose, I suggest you add a reminder to your calendar so you can create a new secret and update the TM Exchange Configuration Utility before it expires.

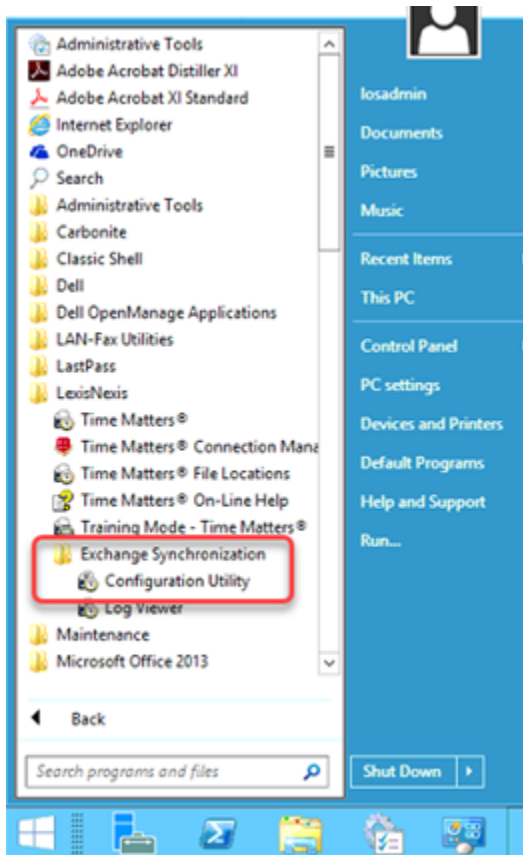
The screenshot shows the 'Add a client secret' dialog box in the Azure Active Directory admin center. The dialog has a title bar with the text 'Add a client secret' and a close button. Below the title bar, there are two main sections. The left section is titled 'Description' and contains a text input field with the value 'Time Matters'. Below this, there is a section titled 'Expires' with a dropdown menu currently set to '24 months'. A list of options is visible: 'Recommended: 6 months', '3 months', '12 months', '18 months', '24 months', and 'Custom'. The right section is titled 'Add' and contains a blue 'Add' button and a grey 'Cancel' button. The background of the admin center is visible, showing the 'Time Matters | Certificates & secrets' page.

Save the “Application Password” value for the TM Exchange Configuration Utility.

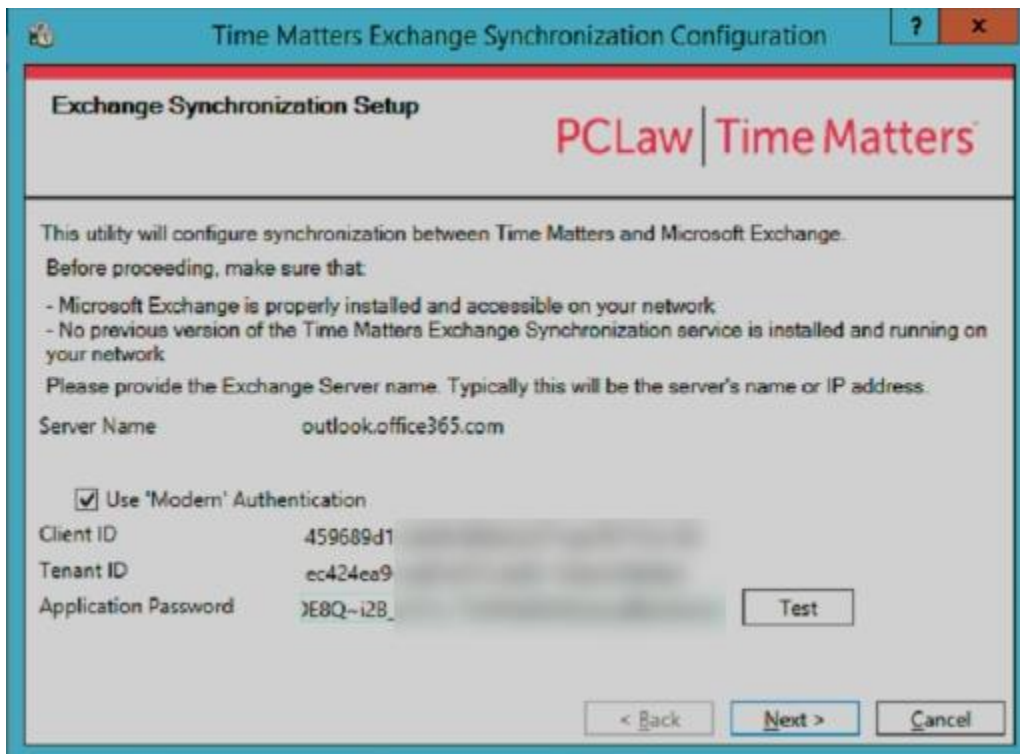
The screenshot shows the 'Client secrets' page in the Azure Active Directory admin center. The page has a title bar with the text 'Client secrets (1)' and a close button. Below the title bar, there is a section titled 'New client secret' with a plus icon. Below this, there is a table with columns 'Description', 'Expires', 'Value', and 'Secret ID'. The table contains one row with the description 'TM Test', the expiration date '10/3/2024', the value 'r8h8Q~...', and the secret ID 'd7608569-...'. A red box highlights the 'Value' column, and a red arrow points from a text box to this value. The text box contains the text 'Enter in TM-Exchange Configuration Utility "Application Password" field'. The background of the admin center is visible, showing the 'Time Matters | Certificates & secrets' page.

Update TM-Exchange “Configuration Utility” settings

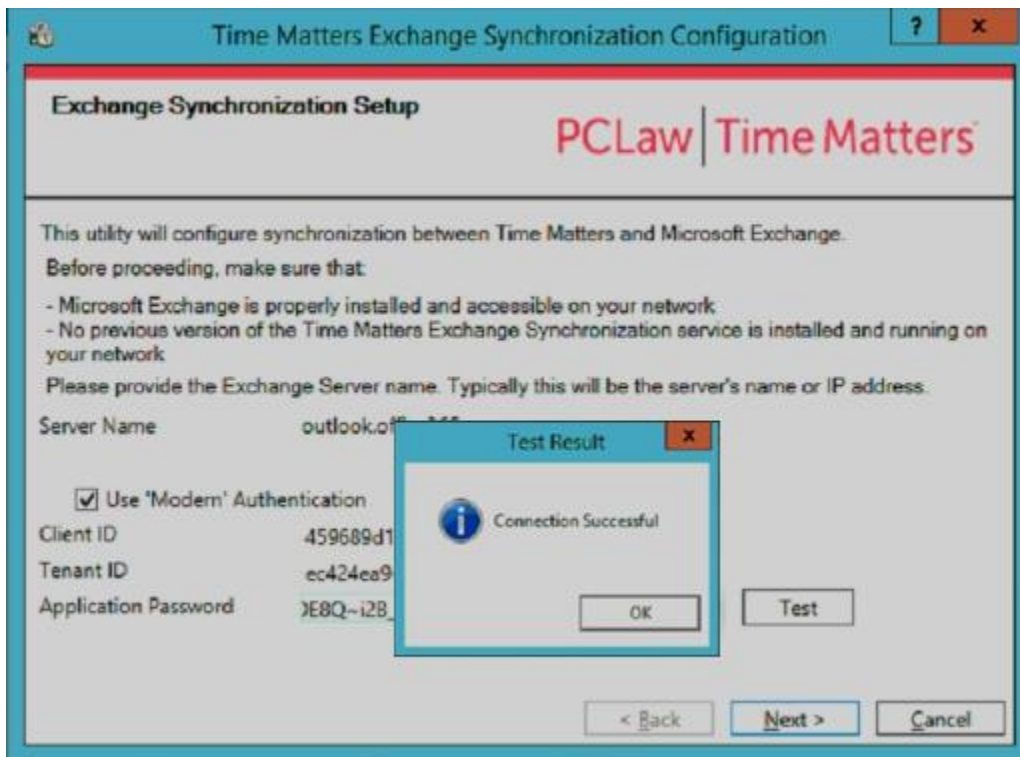
Launch the “Configuration Utility” from the Windows Start left menu.



Enter the 3 values saved in various steps above, and click <Test>



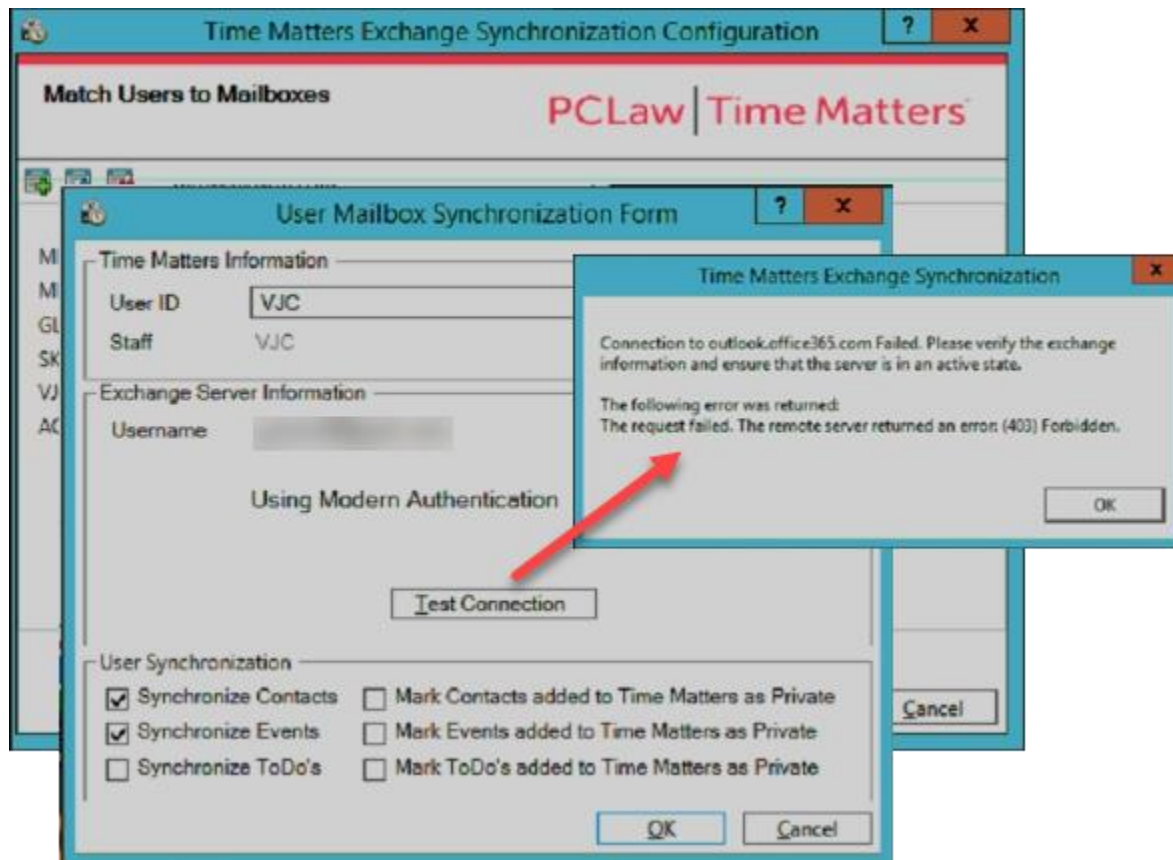
You should get a "Connection Successful" result.



Setup App Permissions - 365 Admin Console

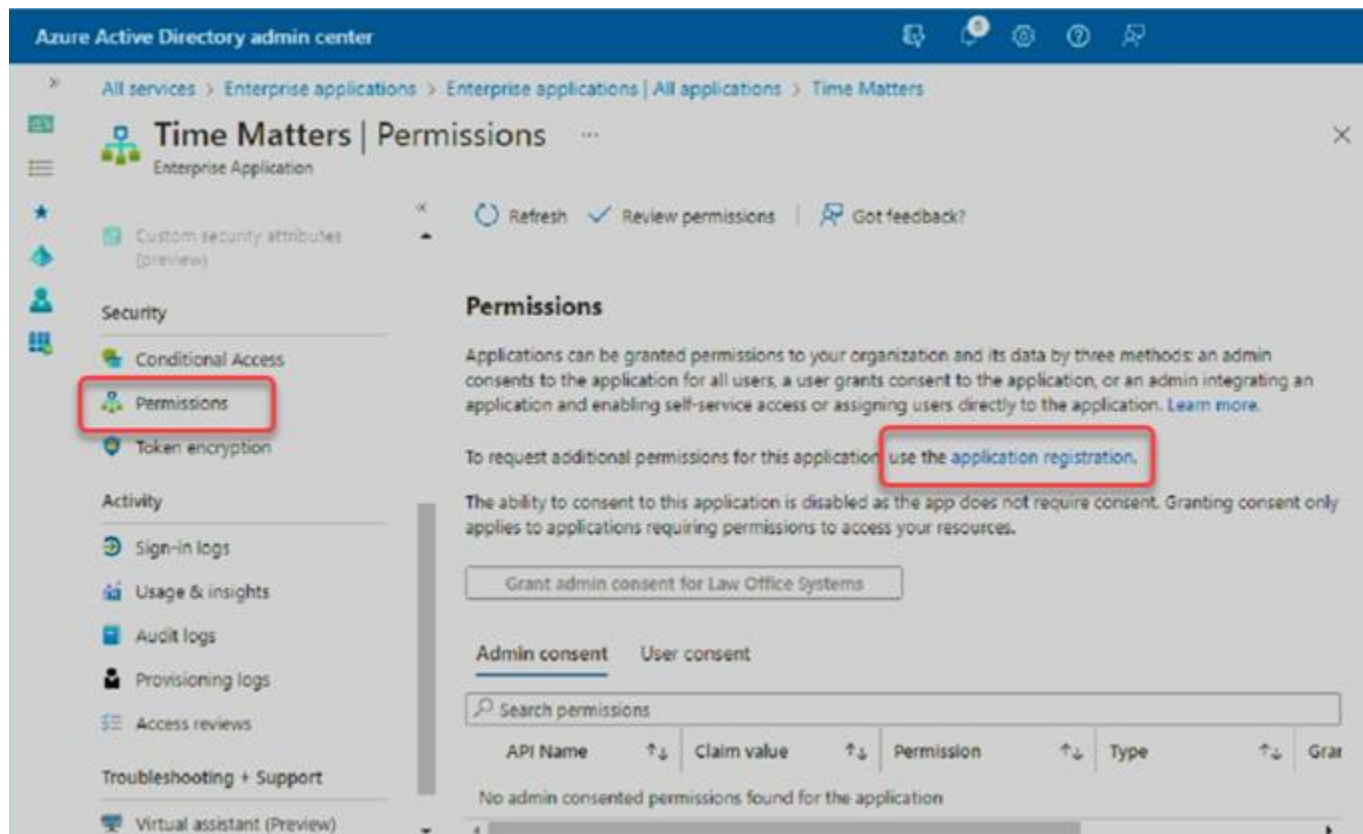
A successful test on the 1st page of the TM Exchange “Configuration Utility” wizard is only a piece of the puzzle. Synchronization fail until permissions are setup properly for the newly added “Enterprise App”. To confirm this, <Next> through the utility pages until you see the list of users on the “Match Users to Mailboxes” page.

Open a user and click <Test Connection> should return an error like this.



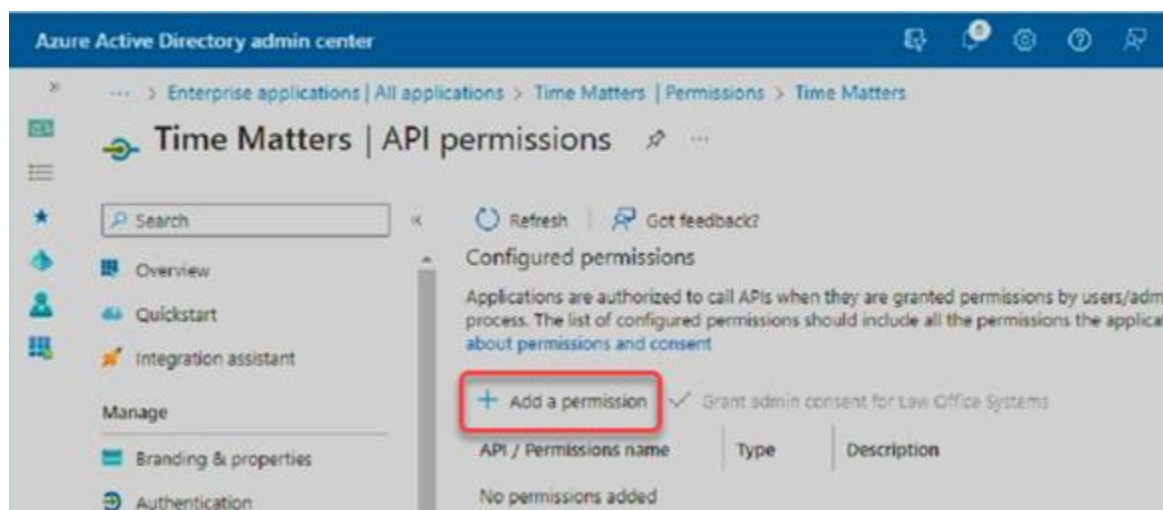
Add Required “Enterprise App” Permissions

If you are still on the “Enterprise application” page for your app, click “Permissions” from the left menu and notice no permissions are listed. Click “Application registration” to jump to the “API permissions” sub-page of the “App registration” page.



Another navigation option is to click “Azure Active Directory” then “App registrations” under the “Manage” section of the left menu. Click <View all applications in the directory> if your TM application entry isn’t visible. Click your TM application in the list, then “API Permissions” in the left menu.

Once on the “API Permissions” page, click “+ Add a permission”.



Click “APIs my organization uses”, type “office 365” in the search field and choose “Office 365 Exchange Online”.

Azure Active Directory admin center

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Search office 365

Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-00
Office 365 Management APIs	c5393580-f805-4401-95e8-9
Office 365 Search Service	66a88757-258c-4c72-893c-3

Choose “Application Permissions” because TM-Exchange sync is an app running as a service, not an actual user.

Find and check the selected permissions as shown here.

Azure Active Directory admin center

Request API permissions

Office 365 Exchange Online
https://ps.outlook.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.

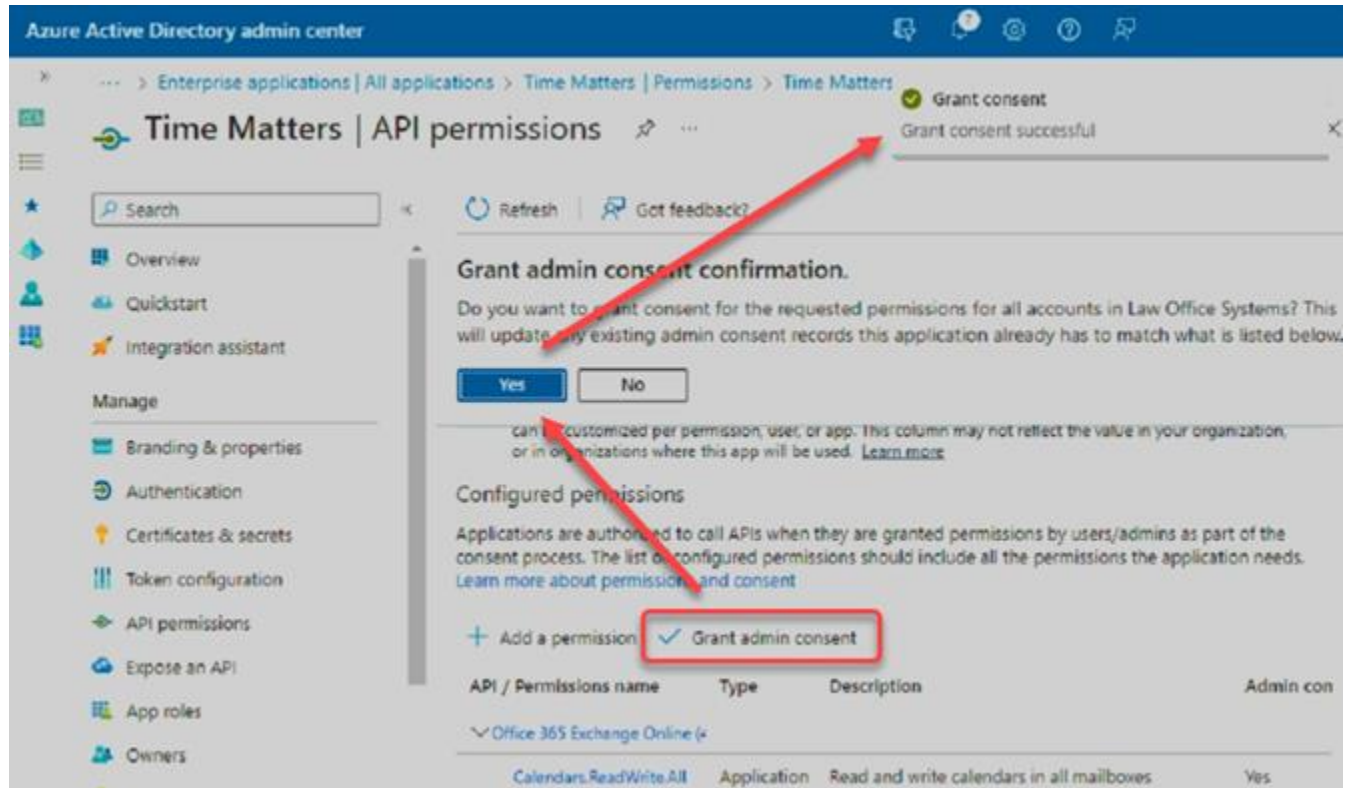
Select permissions

Start typing a permission to filter these results

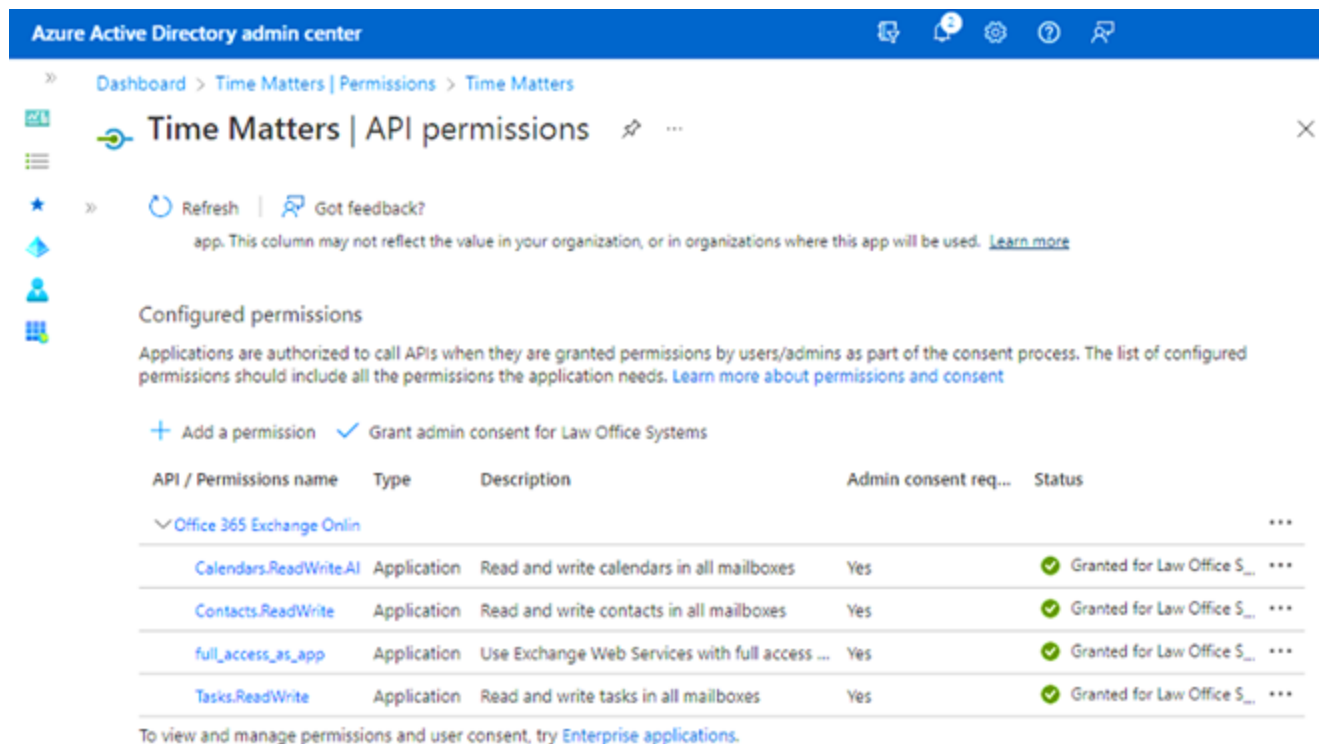
Permission	Admin consent required
Other permissions (1)	
<input checked="" type="checkbox"/> full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Yes
Calendars (1)	
<input type="checkbox"/> Calendars.Read ⓘ Read calendars in all mailboxes	Yes
<input type="checkbox"/> Calendars.Read.All ⓘ Read calendars in all mailboxes	Yes
<input checked="" type="checkbox"/> Calendars.ReadWrite.All ⓘ Read and write calendars in all mailboxes	Yes
Contacts (1)	
<input type="checkbox"/> Contacts.Read ⓘ Read contacts in all mailboxes	Yes
<input checked="" type="checkbox"/> Contacts.ReadWrite ⓘ Read and write contacts in all mailboxes	Yes
Tasks (1)	
<input type="checkbox"/> Tasks.Read ⓘ Read user tasks in all mailboxes	Yes
<input checked="" type="checkbox"/> Tasks.ReadWrite ⓘ Read and write tasks in all mailboxes	Yes

[Add permissions](#) [Discard](#)

The permissions have been added but an Admin must still grant permission to activate them.
Click “Grant Admin consent”, then <Yes>, and look for the “Grant consent successful” message.

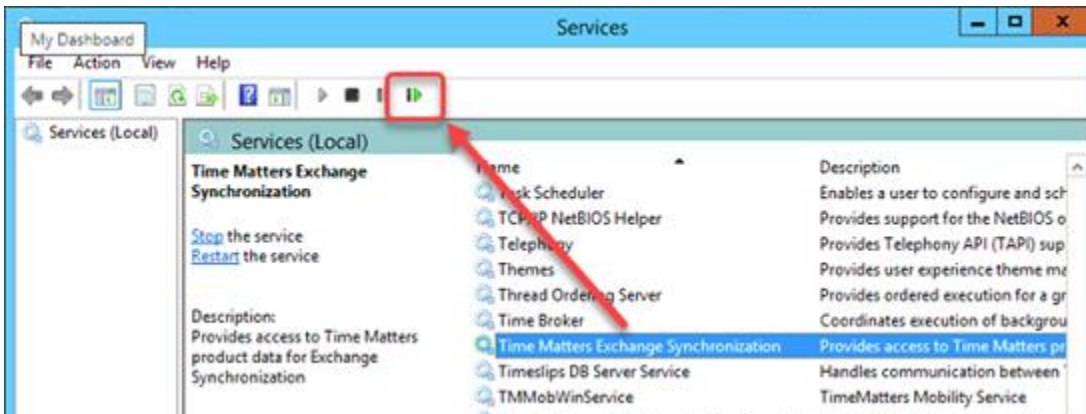


Here’s what the permissions should look like once setup is complete.



Restart the “Time Matters Exchange Synchronization” Service – Local Server

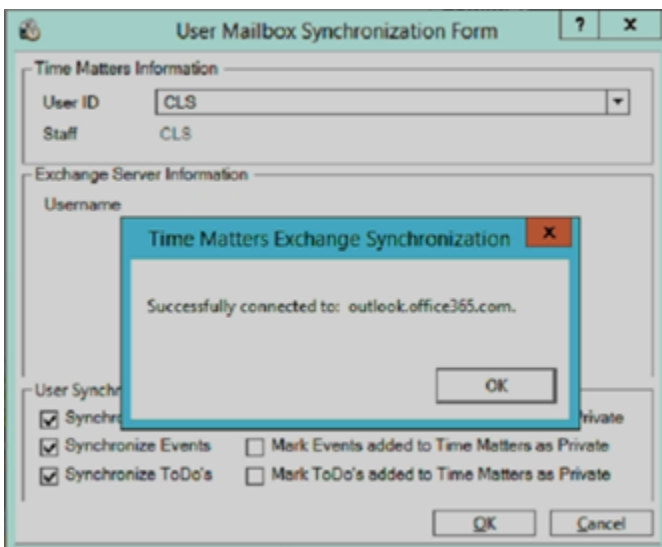
Run the “services.msc” applet on the server where the your “Time Matters Exchange Synchronization” service is installed. Select the service and click the Restart icon, Or click Stop, wait, then click Start.



Test the connection from a specific user from the TM Exchange “Configuration Utility”

Open the “Configuration Utility”, <Next> through the utility pages until you see the list of users on the “Match Users to Mailboxes” page.

Open a user and click <Test Connection> should return a success message like this.



Confirm synchronization is working properly

NOTE: It takes the TM-Exchange sync process a while to catch up after it's been offline for a while. This could be minutes, hours or overnight, depending on how much data there is to update. How much time is impacted by size of the firm, activity level and amount of time the sync was offline. Be patient if you don't see records appearing right away. Check back in an hour, or possibly the next morning for larger firms.

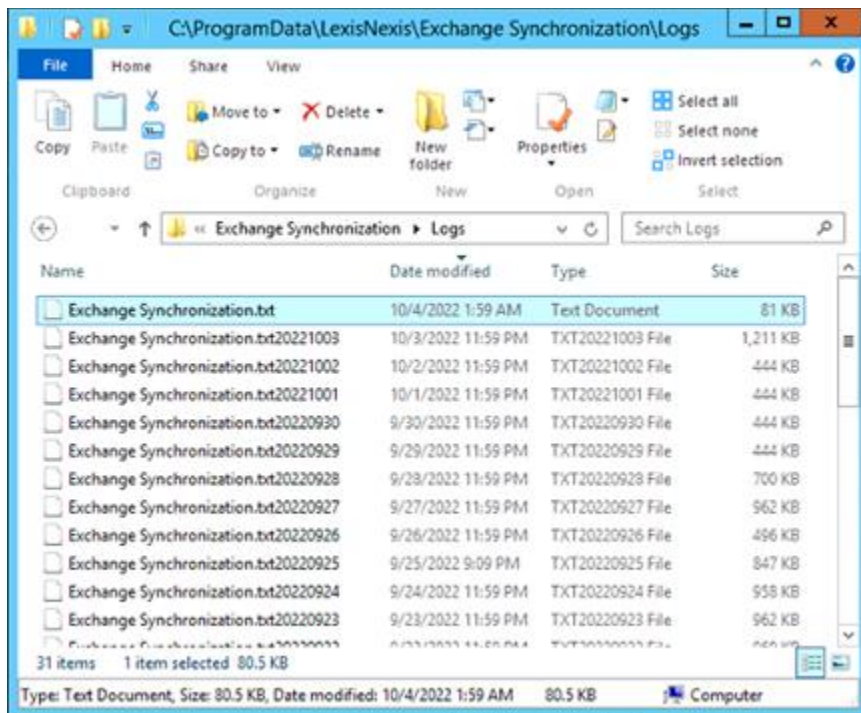
Each time the "Time Matters Exchange Synchronization" service is restarted the schedule prepares to sync in 60 seconds.

All sync activity is saved to a log file named "Exchange Synchronization.txt" here:

"C:\ProgramData\LexisNexis\Exchange Synchronization\Logs"

Open this log in Notepad and scroll to the bottom to see the latest activity. Pay attention to the date and time stamps on each line to navigate the content.

As the log fills up the system renames the log file adding a datestamp, then creates a new "Exchange Synchronization.txt" file on the next activity event. For example:



If the log file becomes too full to easily navigate you can stop the service, manually rename the current log and restart the service. Now the log file will only contain current sync activity.