

Email service based on App Registration Instructions for Office365 (aka Exchange Online)

Complete the following instructions to find the values to enter into the Directory (Tenant) ID, Application (Client) ID, Client Secret Value, and Authority fields in the Email Manager option in the School Accounting System, as shown below, for use with OAuth2 authorization. Once the values have been determined, access the Email Manager option under the Maintenance menu on the main School Accounting System screen.

Enable Email Manager ☒

Use Hosted Mail Server ☐

General Information

Enable SSL ☐

Mail Server

Port Number

Email Message Font

Disclaimer Font

Disclaimer

Send Emails in Groups ☐

Number of Emails per Group

Pause Between Groups (Minutes)

Directory (Tenant) ID

Application (Client) ID

Client Secret Value

Authority

Report Options

Default Email Address ID

Backup Options

Send Email Notification ☐

To Email Address

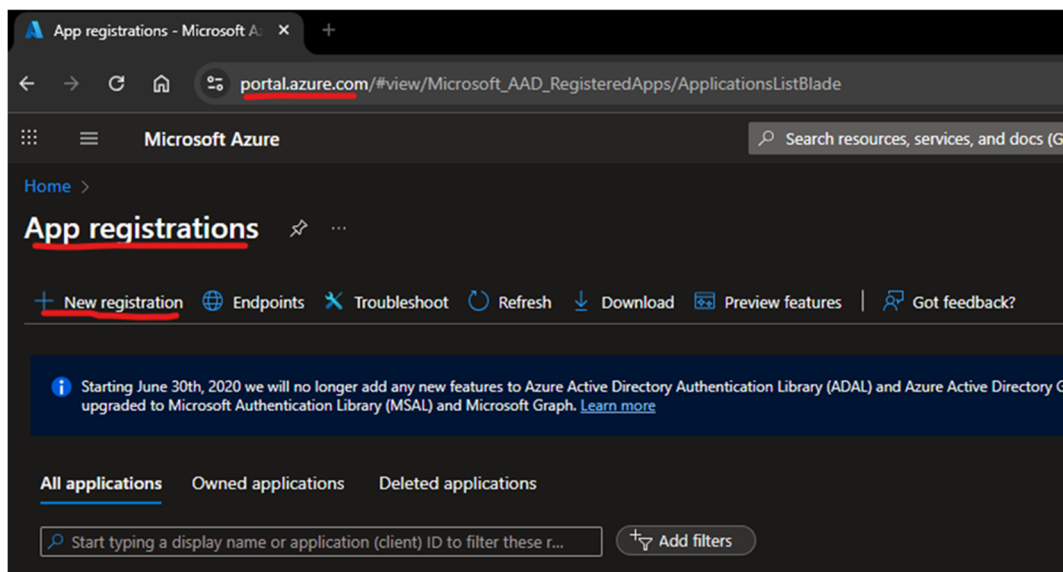
Email Address ID

Pre-requisites(s):

- User who is Global Administrator in the Azure (aka Microsoft/Office 365) Tenant.
- Email account(s) within the Tenant that is going to be used as the “from” address for emails sent from the School Accounting System. Shared mailboxes are allowed to be used.

Instructions:

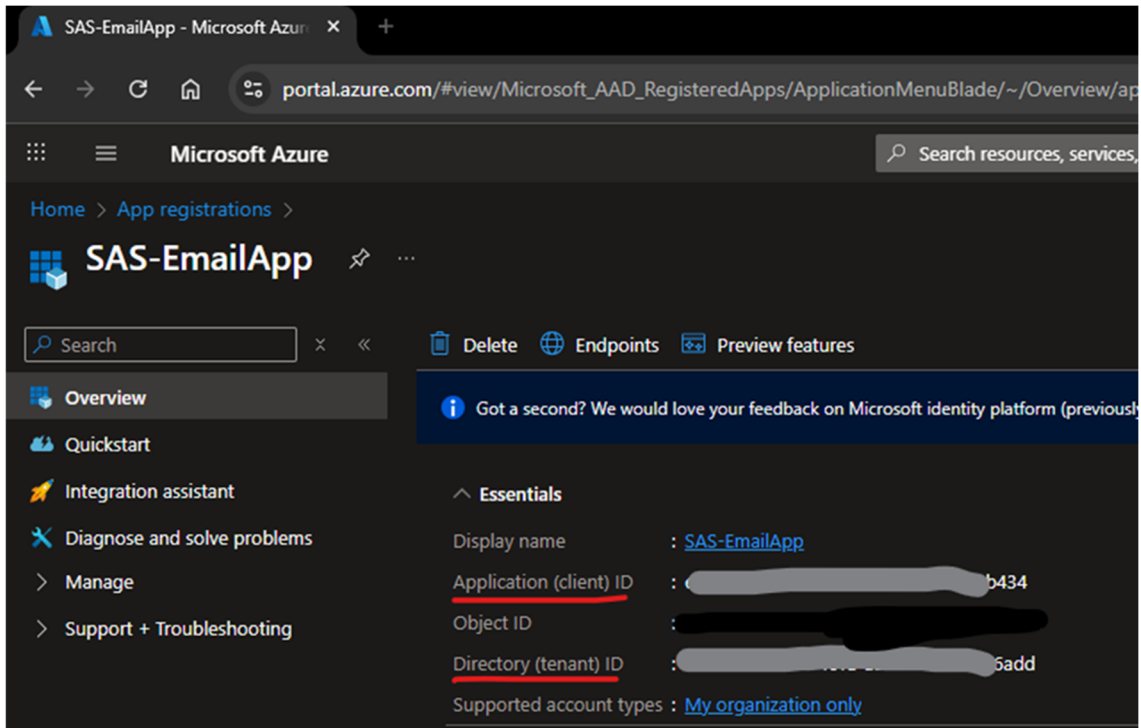
- 1) Go to <https://portal.azure.com> -> Log In with Global Admin user.
- 2) Search for “App Registrations”.
- 3) Select “+ New Registration”.



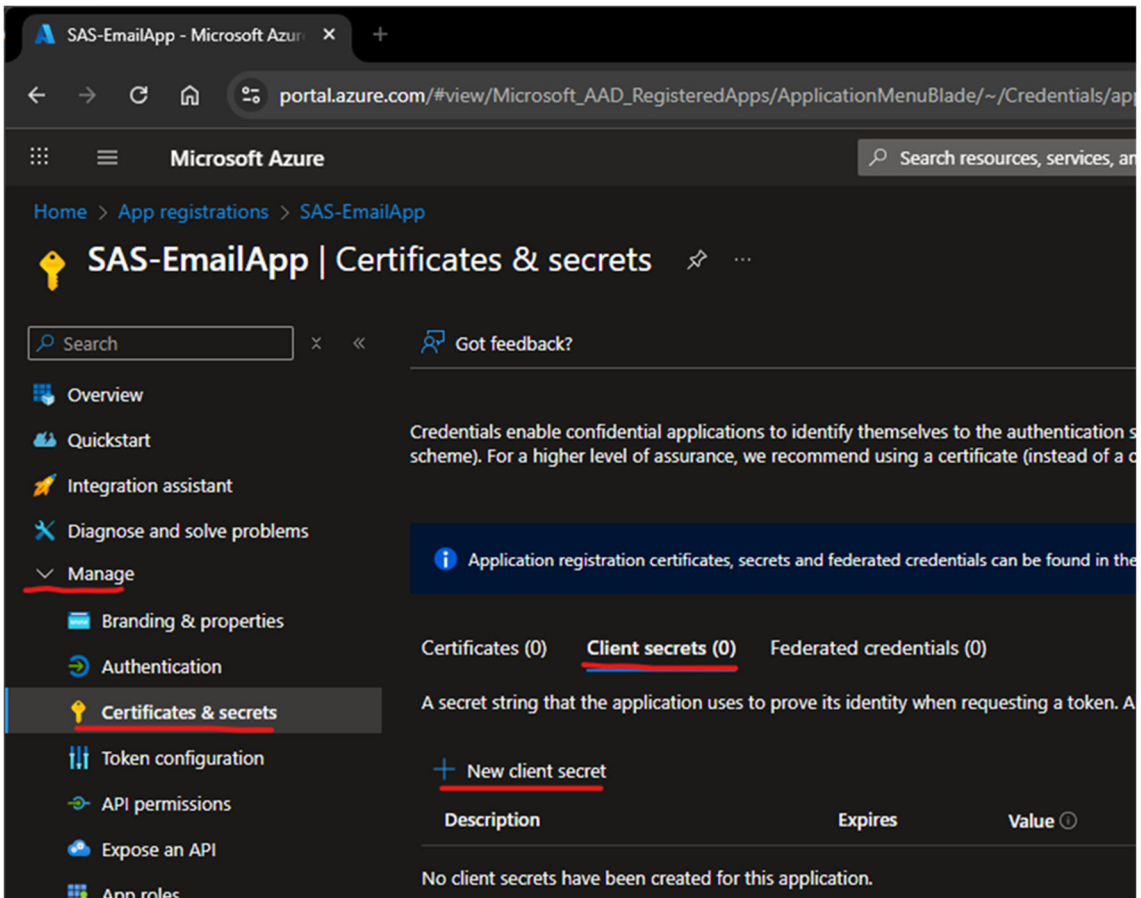
- 4) Create a Name for the app, leave the default selection of “Accounts in this organizational directory only”, and select “Register”.

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The browser address bar shows 'portal.azure.com/'. The page title is 'Microsoft Azure'. The breadcrumb navigation is 'Home > App registrations >'. The main heading is 'Register an application'. Below this, there is a section for 'Name' with a description: 'The user-facing display name for this application (the name that appears in the app's user interface)'. The text 'SAS-EmailApp' is entered in the input field. Below the name field is a section for 'Supported account types' with the question 'Who can use this application or access this API?'. There are four radio button options: 'Accounts in this organizational directory only (Recommended)', 'Accounts in any organizational directory (Any Azure AD directory - Single sign-on)', 'Accounts in any organizational directory (Any Microsoft account - e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. The first option is selected. Below this is a link 'Help me choose...'. Further down is a section for 'Redirect URI (optional)' with a description: 'We'll return the authentication response to this URI. This URI is optional and it can be changed later, but a value is required for most applications'. There is a dropdown menu for 'Select a platform' and a text input field for the URI with a placeholder 'e.g. https://'. Below this is a link 'Register an app you're working on here. Integrate with your app'. At the bottom, there is a link 'By proceeding, you agree to the Microsoft Platform Terms of Service' and a blue 'Register' button.

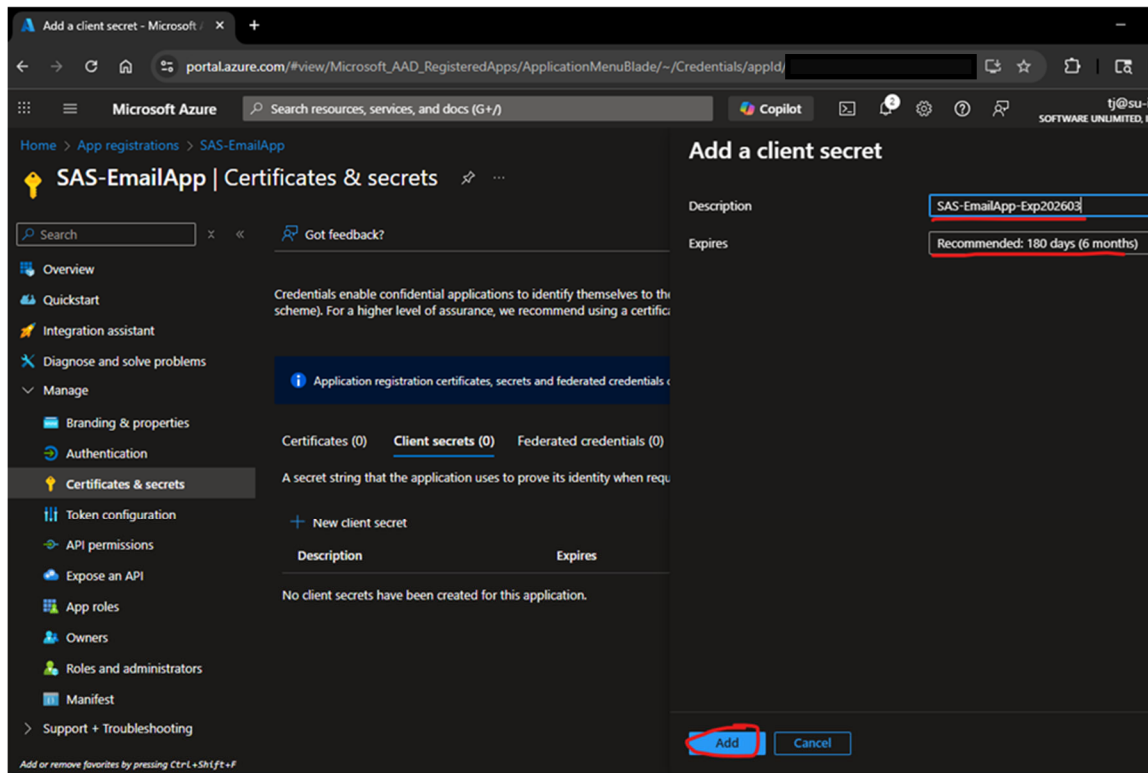
- 5) Save the “Application (client) ID” and “Directory (tenant) ID” for entry into the School Accounting System. This information can be viewed in Azure later if needed. It is hidden in the picture as it could be sensitive information, and should not be accessible by the public.



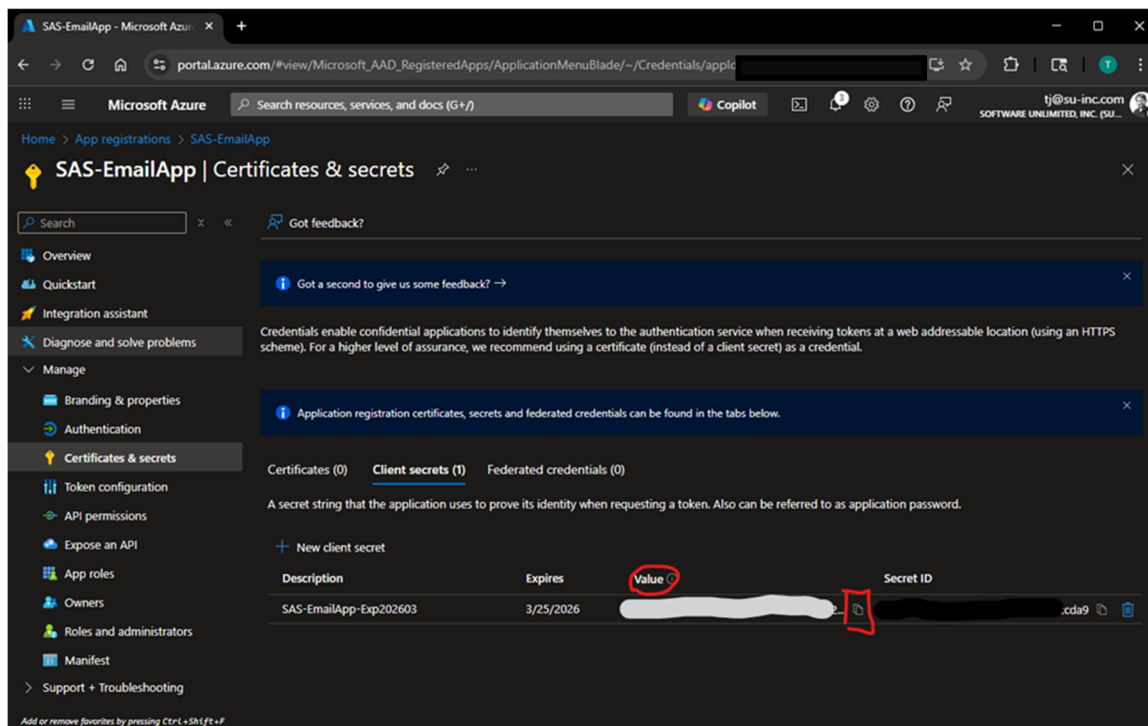
- 6) Expand the “Manage” menu in the left navigation bar, select “Certificates & secrets”, select the “Client secrets” tab, and select “New client secret”.



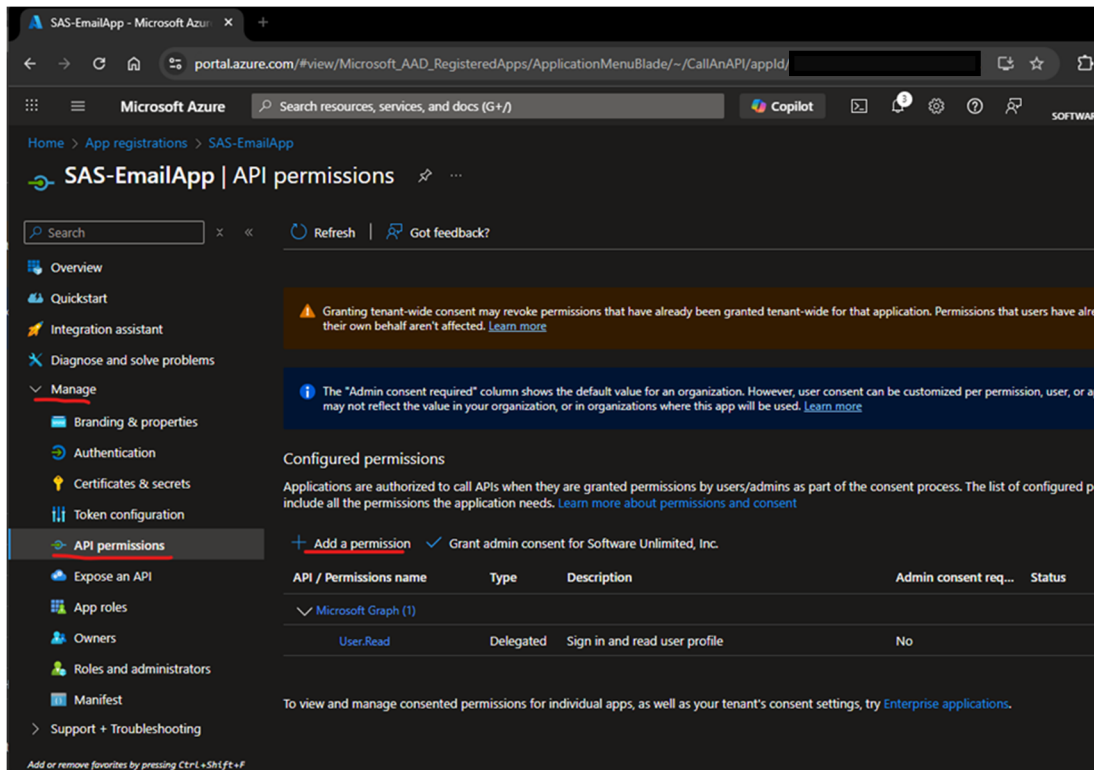
- 7) Create a Description for this secret, select an expiration timeline (current options range from 3 months to 24 months), and select “Add”. Please note that this secret will need to be updated before expiration to continue facilitating email service. New secrets can be created anytime before expiration.



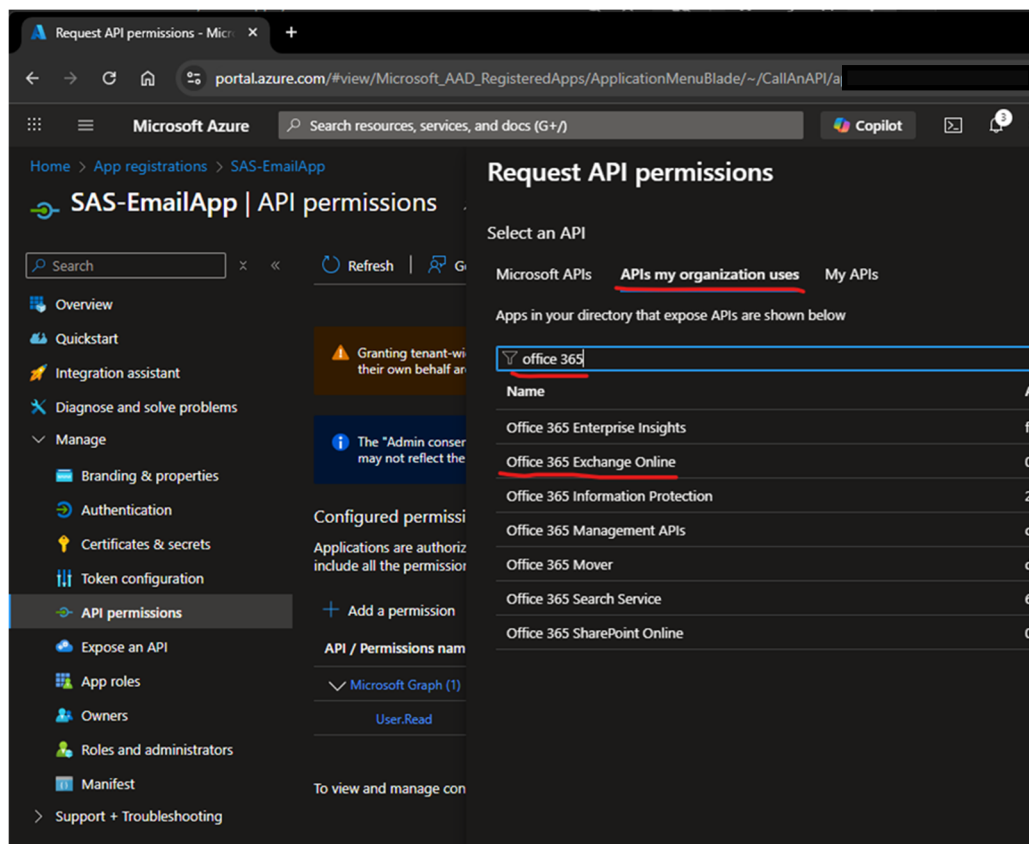
- 8) Copy the “Value” string from this Client Secret into the Client Secret Value field in the School Accounting System. There is a “copy” icon on the right of the secret value. This value should be protected from unauthorized access.



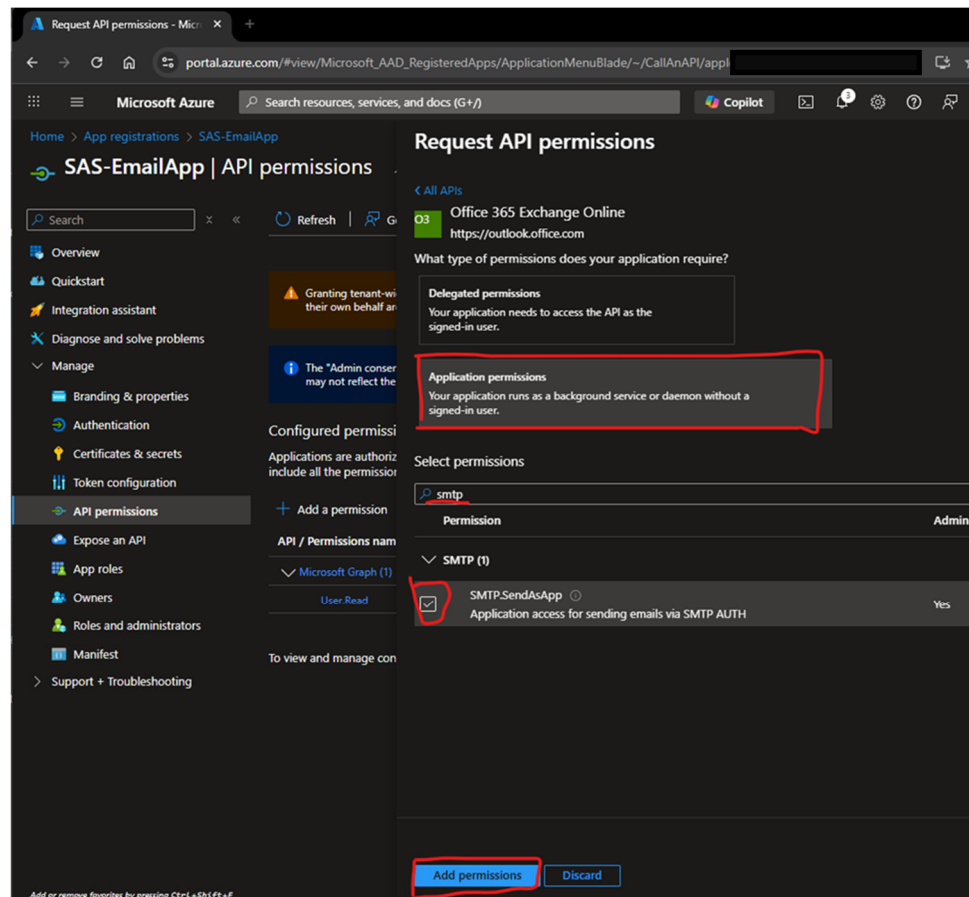
- 9) Now select “API Permissions” from the “Manage” menu in the left navigation bar, and then select “Add a permission”.



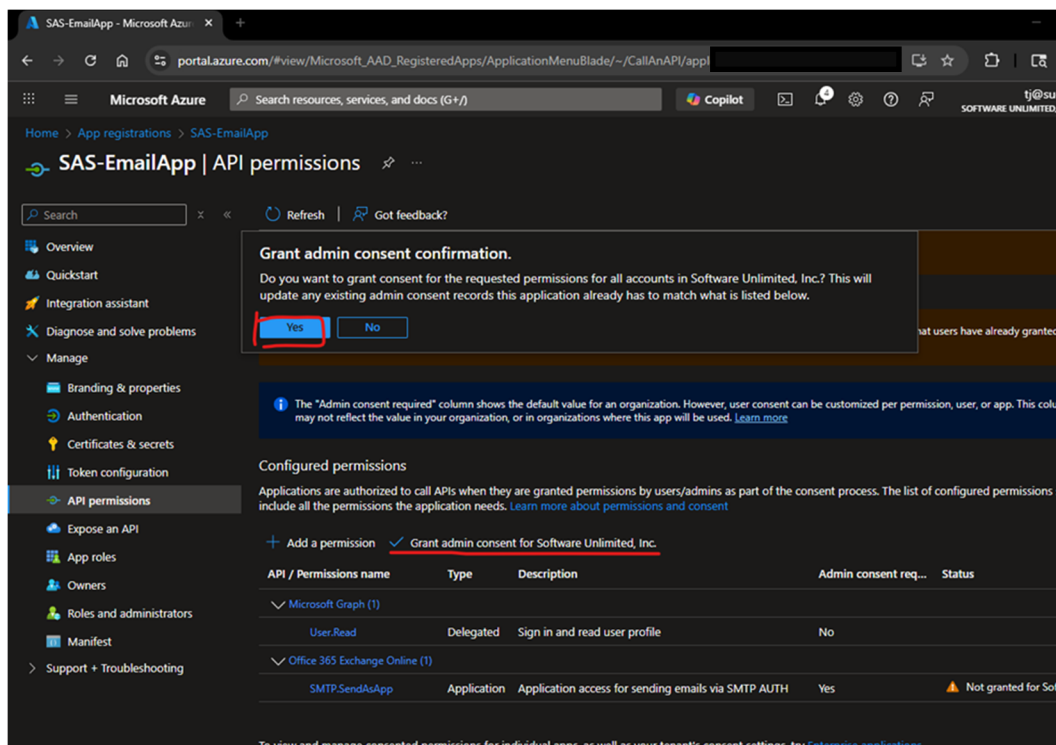
- 10) Select “APIs my organization uses”, type “office 365” to narrow the list, and select “Office 365 Exchange Online” from the options.



- 11) Select “Application permission”, type “smtp” to narrow the list, select “SMTP.SendAsApp” from the menu and select “Add permission”.



- 12) Select “Grant admin consent for {Your organization name}” and then select “Yes”.



13) The Granted icons should turn green:

consent req...	Status
	...
✓	Granted for Software U... ..
	...
✓	Granted for Software U... ..

14) Select the “Cloud Shell” icon and enter: “Import-Module ExchangeOnlineManagement” and then “Connect-ExchangeOnline”.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Cloud Shell' icon, which is highlighted with a red square. Below the navigation bar, the page title is 'SAS-EmailApp | API permissions'. The left sidebar contains a menu with options like 'Overview', 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage', 'Branding & properties', 'Authentication', and 'Certificates & secrets'. The main content area displays a message: 'Successfully granted admin consent for the requested permissions.' Below this, there are two informational messages: one about granting tenant-wide consent and another about the 'Admin consent required' column. At the bottom of the portal view, a Cloud Shell terminal window is open, showing the following commands and output:

```
PS /home/tj> Import-Module ExchangeOnlineManagement
PS /home/tj> Connect-ExchangeOnline

-----
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these
f WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

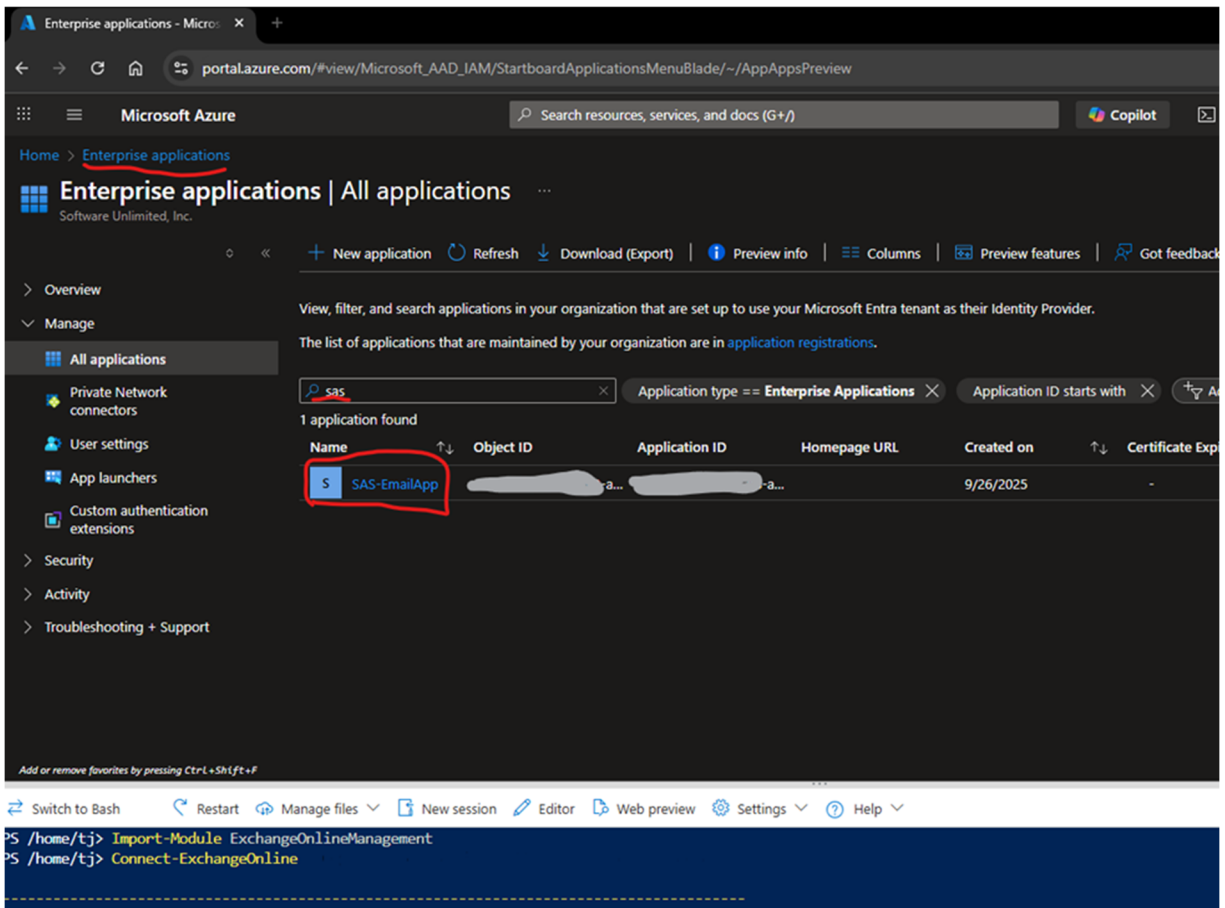
V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

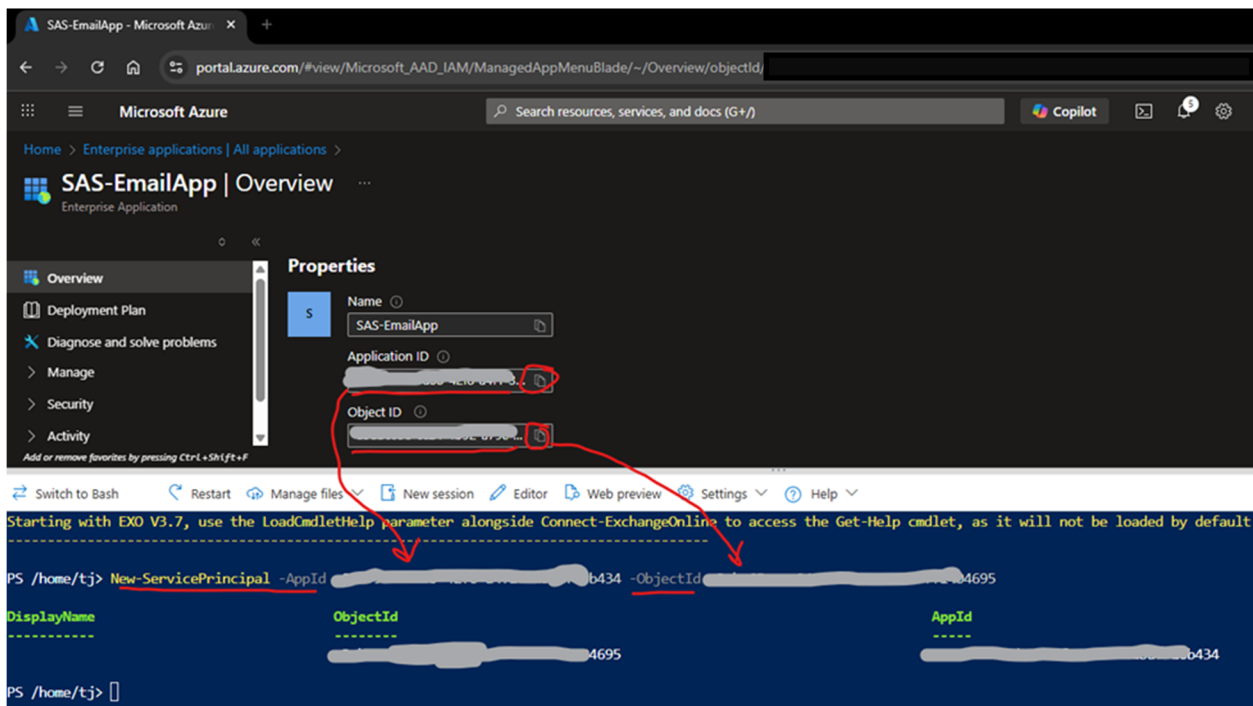
Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmdlet, as it will not be loaded by default
-----
PS /home/tj> 
```

15) Without closing the Cloud Shell, in the search, type “Enterprise App...” and select “Enterprise applications”, search for the app name to narrow the list, and select the App created above.



- 16) Type "New-ServicePrincipal -AppId " and then copy the Application ID and right click "paste as plain text", and then type "-ObjectId " and copy and "paste as plain text" and then press enter. The command should resemble this:

>New-ServicePrincipal -AppId <APPLICATION_ID> -ObjectId <ENTERPRISE_APP_OBJECT_ID>



17) Type "Get-ServicePrincipal | fl" and find the "ExchangeObjectId" of the service principal just created.

```
WhenCreated          : 9/26/2022
WhenChangedUTC       : 9/26/2022
WhenCreatedUTC       : 9/26/2022
ExchangeObjectId     : 9e847374
```

18) To allow permission, use this ID and the mailbox you want to 'Send As'. (Please be advised that emails sent "from" this application will appear to be "from" the account(s) enabled in these steps. It may be advisable to create a dedicated email address just for this application. Shared mailboxes are also allowed to be used.) You may enable multiple email addresses/shared mailboxes (e.g. payroll@, ap@, etc.).

Add-MailboxPermission -Identity "sender@yourdomain.com" -User <EXO_ServicePrincipal_Identity> -AccessRights FullAccess

```
PS /home/tj> Add-MailboxPermission -Identity "K...@su-inc.com" -User 9e847374 -AccessRights FullAccess

Identity      User      AccessRights
-----
K...@su-inc.com  S-1-5-... {FullAccess}

PS /home/tj>
```

19) Ensure SMTP Auth is allowed for the mailbox by entering:

Set-CASMailbox -Identity sender@yourdomain.com -SmtpClientAuthenticationDisabled \$false

```
PS /home/tj> Set-CASMailbox -Identity "K...@su-inc.com" -SmtpClientAuthenticationDisabled $false
PS /home/tj>
```

20) For the Authority Section, enter this string replacing <Tenant_ID> with your Directory (tenant) ID above:

https://login.microsoftonline.com/<TENANT_ID>/v2.0 (remember to remove the "<" and ">")

21) Ensure email addresses in the School Accounting System are enabled in this process, and add the IDs created above to the appropriate fields on the General Options tab in Email Manager, and test sending from email addresses added in here and also confirm that addresses not added in steps 18 and 19 result in an error message.

22) **Tip:** Set a reminder for the expiration of the Client Secret – a little while before it expires you can create an additional secret with a new expiration and replace the existing one without any disruption of service.