BRTSys

USER GUIDE

PanL Desk Manager 3.1.0

Part 2 – Installation and Configuration

Document Version: 2.0

Issue Date: 01-07-2024

Table of Contents

1. About This Guide

This guide explains the Installation/Setup & Configuration of PDM Server, Mail/Calendar Server. **The screenshots used are for illustration purposes only**.

2. Intended Audience

The intended audience are System Integrators, Technical / Administrative users who will assist in realizing the capabilities, functions, and the full benefits of the product.

Note:

1. Ensure the firmware version and package version number are up-to-date and update/upgrade accordingly.
2. For more information about the latest version and compatibility, contact the BRT Systems sales/support.

3. Document References

Document Name	Document Type	Format
BRTSYS_AN_044_PDM User Guide - 1. Introduction	Application Note / User Guide	PDF
BRTSYS_AN_046_PDM User Guide - 3. PDM Management Console and Desk Viewer		
BRTSYS_AN_047_PDM User Guide - 4. Mobile Client App and PanL PD35L Display		
BRTSYS_AN_048_PDM User Guide - 5. Outlook Add-In		

4. PDM Server Installation & Configuration

4.1 Hardware / Software Requirements

Hardware / Software	Specifications		
Server Operating System	Ubuntu LTS 18.4+ / CentOS Stream 9+ / SUSE 15.5+ / RHEL 8.6+		
Exchange Server	Microsoft Exchange 2013/2016/2019 & Microsoft 365		
Database Software	MongoDB 4.2.0		
PDM Management Console Web Browser	Mozilla Firefox v69+/Chrome v65+/Safari		
Client Software	Outlook Add-In 2010/2013/2016/Outlook App Ensure that any of the above outlook versions are installed.		
Minimum Server Hardware Requirements	Processor –Intel i7		
	Hard disk – 50GB		
	RAM – 4GB RAM		
Network Ports	Exchange Server	Port 443	Used for EWS connection
		Port 587	Used for SSMTP
	PDM Server	Port 9881	Used for PDM Management Console
		Port 3000 / Port 443	Used for API
		Port 3002	Used for Socket Notification
		Port 3001/ Port 65533	Used for PanL PD35L Device
	Client (Outlook Add-Ins)	Port 3000/ Port 3002	Used for API and socket notification
	PanL35L	Port 3001/ Port 65533	Used for PDM API
	Mobile Client	Port 3000/ Port 443/ Port 3002 Port 5353	Used for API, Socket Notification and mDNS
	Desk Viewer	Port 9881	

Table 1 - Hardware / Software Requirements

4.2 Network Port Requirements

If your infrastructure has Firewall, ensure that the following ports are not blocked –

Source	Destination	Ports
PDM Server	MS Exchange Server / Microsoft 365	443, 587
PanL PD35L Outlook Add-in Mobile app Desk Viewer	PDM Server	443, 3000, 3001, 3002, 5353, 9881, 65533

Table 2 – Network Port Requirements

4.3 Installing PDM on Linux-Distribution Server

Note: This section is applicable ONLY for SUPERADMIN Users

4.3.1 System Requirements

- A static IPv4 address (assigned to PDM Server IP).
- A user account with "sudo-able" full permissions
- Access to the internet during installation to download dependencies. (optional)

4.3.2 Pre-Installation Procedure

Note: For CentOS, RHEL and SUSE systems, administrators must explicitly open port 5353 by executing the following commands with sudo privileges:

```
firewall-cmd –zone=public –add-port=5353/tcp –permanent
firewall-cmd —reload
```

Installation and configuration of the PDM Server Software and its components are described in this section. **The screenshots and file names used are for illustration purposes only**.

- Copy the PDM installation package zip file provided (for example **– *PDM_package_3.0.0-2.1.0-P.zip***) to the PDM Server PC (for example: */home/bridgetek/PDM/*)
- Unzip or extract the installation files using the following command **–**

```
unzip PDM_package_3.0.0-2.1.0-P.zip -d PDM_package_3.0.0-2.1.0-P
```

- Upon extracting the package file, the PDM package folder is displayed.

- Double click to open the PDM package folder to view the list of subfolders and files –

4.3.3 Installing PDM Server Software

The steps to install the PDM Server Software are given below.

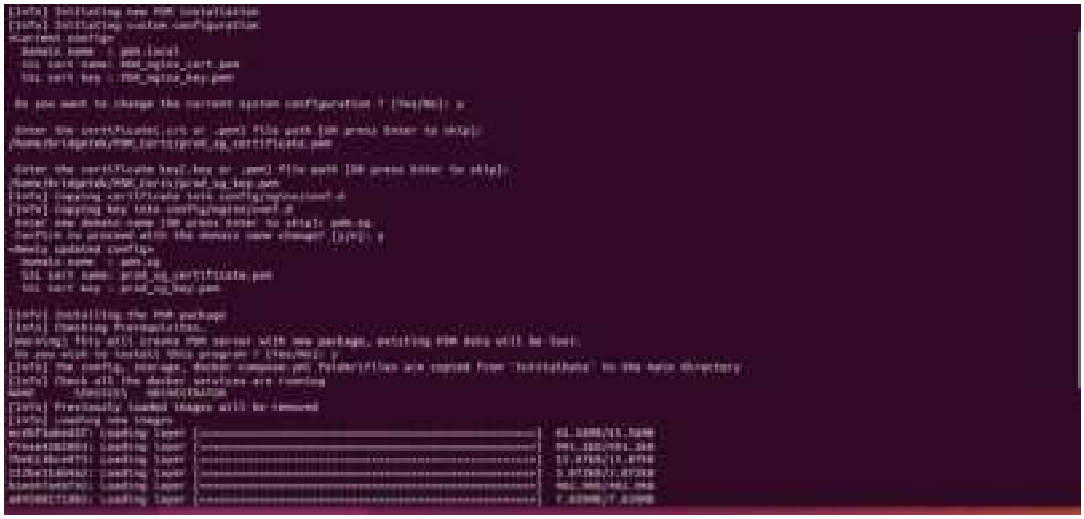
- Open a terminal / command prompt from the package directory *(for example – PDM_package_3.0.0-2.1.0-P)* and enter the following command to provide the execution permission for the script files.

```
$ sudo chmod -R +x *.sh
```

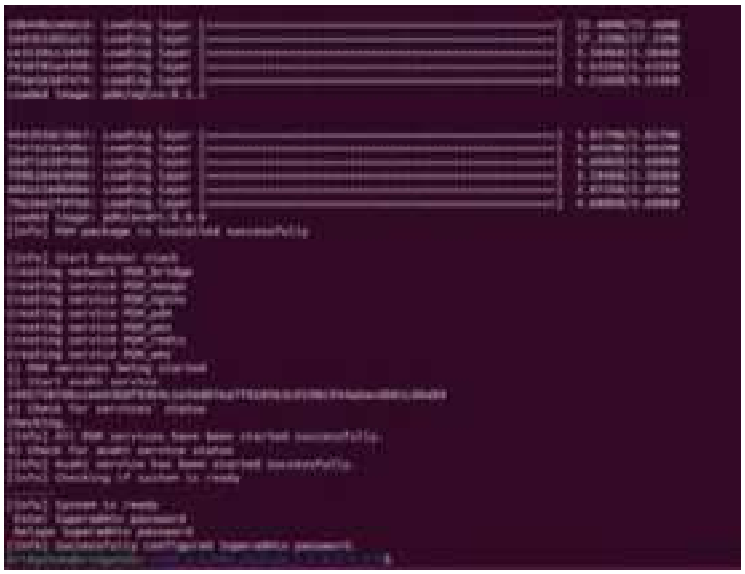
- Run the following command to install the software –

```
$ sudo ./PDM_setup.sh
```

- Upon running sudo ./PDM_setup.sh, user will be prompted, to change the SSL Cert and Domain Name from the default configuration. If user chose *"yes"*, then, the user must enter the certificate path, certificate key path, and the new domain name.



- The user will be prompted to enter a superadmin password at the end of the installation.



4.3.4 Update PDM Server Software Package

The steps to update the PDM Server Software are given below. **The screenshots used are for illustration purpose only**.

- Extract the new package and go to the **new package directory** path using the following command **–**

  ```
  $ cd PDM_package_3.0.0-2.1.0-p/
  ```

- Run the following command to change mode **–**

  ```
  $ sudo chmod -R +x *.sh
  ```

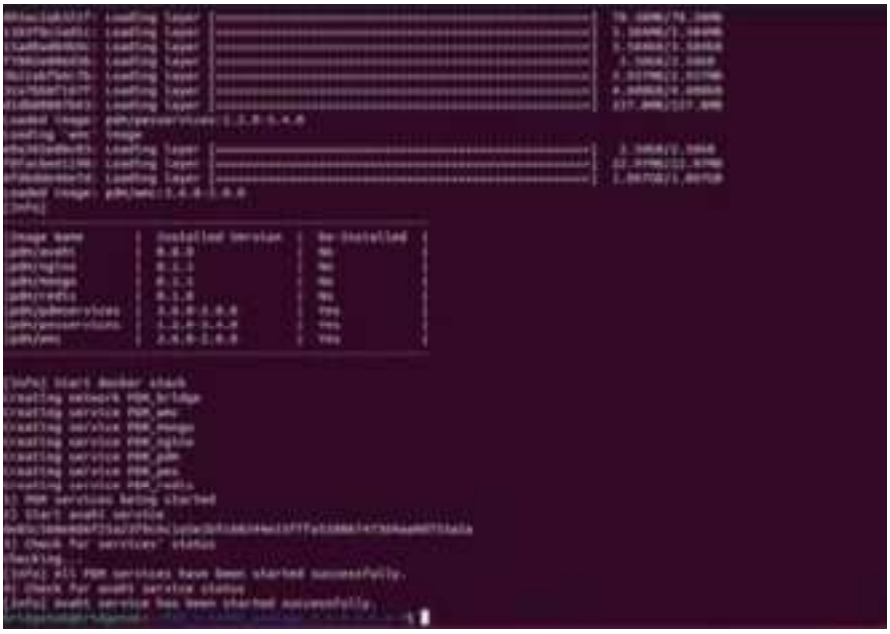
- Run the following command to update the package **–**

  ```
  $ sudo ./PDM_setup.sh
  ```

- A list of options for installing updates are displayed. Choose one of the three options by entering 1 / 2 / 3 accordingly.

  Enter **1**, to use the setup configuration from previously installed package (enter the old software package directory path to retain all previous PDM Server and PDM Management console

configuration data); Enter **2**, to apply the new package's setup configuration; Enter **3**, to configure manually. For illustration purpose, option **1** is used.



- Upon successful update, the difference between old and new component versions is displayed as specified in table.

4.3.5 Change the current SSL Certificate and Domain Name

The steps to change the current PDM Configuration is given below. **The screenshots used are for illustration purpose only**.

- Changing the current configuration for **–**
  - SSL Certificate
  - Domain Name for PDM Server
- For changing certificate, your certificate must be generated using the PDM Server IP Address.
- Use the following command to change certificate or domain name **–**

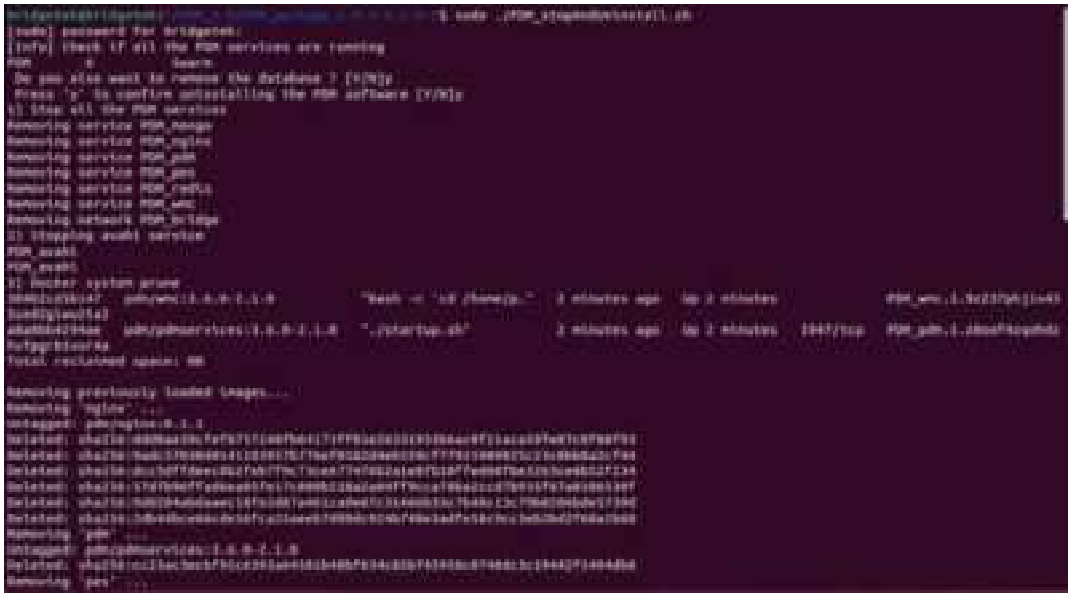
```
$ sudo ./PDM_configure.sh
```

4.3.6 Un-install PDM Server Software Package

The steps to un-install PDM Server Software Package are given below -

- To un-install PDM Server software package, use the following command –

```
$ sudo ./PDM_stopAndUninstall.sh
```



- If you want to remove the database, enter **Y**. Selecting yes, will remove your previous database and this will be equivalent to a fresh installation.

Note: It is recommended to back up the configuration data (PDM Management Console > Settings > Import / Export Configuration > Export) before performing any uninstallation operation. If required, you can restore the exported configuration.

4.4 Domain Name Configuration

After the PDM Server Software installation, the network administrator MUST configure the DNS to resolve the following Domains:

- ✓ app.<your_domain_name>
- ✓ api.<your_domain_name>
- ✓ socket.<your_domain_name>

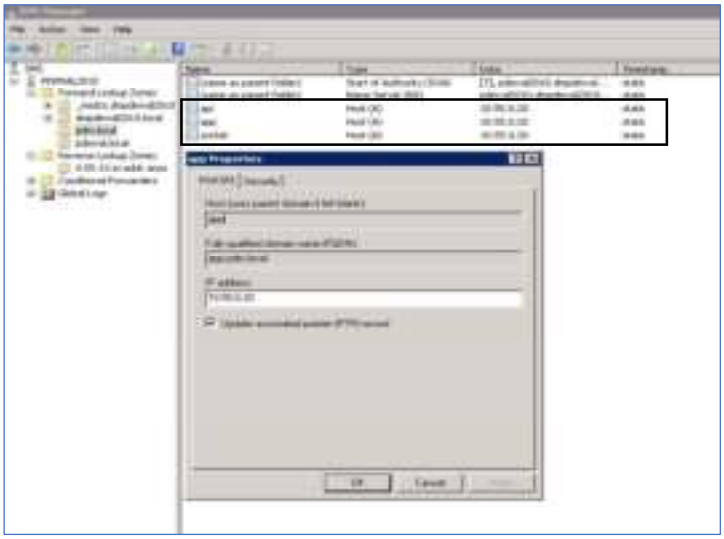
where in the *domain name* refers to the *organization's domain name*. For example, if the organization's name is ABC Pte Ltd, then the domain name can be abc.com or abc.local.

The DNS records can be created/added in the following ways –

- Local DNS Server
- Global DNS Service

Local DNS

To configure the domains on a local DNS server, ensure the DNS records are created in the exchange server. For illustration purpose exchange server 2010 is used in the example below –



Global DNS

To configure a public domain on a purchased GLOBAL DNS host server (*for example GODADDY*), create the DNS records as shown in the picture below-

4.5 SSL Certificate Setup

There are two types of SSL certificates that can be installed on a PDM Server **– self-signed** and **public CA** certificates. This is configured during installation and can be updated at runtime by using *PDM_configure.sh*.

Use of self-signed certificate

Certificates generated for the PDM Server must have a validity period of no more than one year, as iOS devices do not accept certificates with expiration dates beyond this timeframe. Consequently, applications on iOS will be unable to establish a connection with the PDM Server if the certificate does not meet minimum validity period.

It is essential for the Subject Alternative Name (SAN) field in the certificate to include both the domain name and the IP address of the PDM Server.

Users are required to install the certificate on their mobile devices to facilitate a connection to the PDM Server. Administrators should distribute the certificate to users, ideally via email, as this method simplifies the installation process for the end-users.

Additionally, when users access the PDM Management Console via web browser, they must acknowledge and accept any security risks presented.

- **Installing self-signed certificate**

  The end users must install the self-signed certificate on their OS.

  For Windows

  Refer to https://learn.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate for installing SSL certificate into Windows Trusted Root Certificate Authority.

  For Mac

  Refer to https://support.apple.com/guide/keychain-access/add-certificates-to-a-keychain-kyca2431/mac for installing SSL certificate into macOS Keychain Access.

Use of public cert

It is mandatory that the Subject Alternate Name record on the certificate contain the domain name.

5. Mail/Calendar Server Setup & Configuration

5.1 Exchange Server 2019/2016 / 2013 Setup

Account Reference	Account Type	Number of Accounts	Description
User Account	User Mailbox	X	This account will be used by the normal end users to perform desk booking related activities.
Distribution Group for Users	Group (Users)	X	This group of users (**pdm-user-group-**<groupname>) are only allowed to access the following PDM components – • PDM Management Console • Outlook Add Ins • PanL PD35L device On spot booking
Resource Account	Desk Mailbox	X	These are accounts associated with the desk resource. • This account will be part of the distribution group.
Distribution Group for Desks	Group (Room List)	X	This group of desks (**pdm-desk-group-**<groupname>) are only recognized as valid resources in the PDM.
Impersonation User / Service Account	User	1	This user will be able to access multiple mailboxes and act as the mailbox owner. This account will be used – • To communicate between PDM and Exchange Server. • All the PDM Server / Desk Booking related emails will be sent by this user • Upon installation of PDM Server, this user account details must be added in the "**PDM Management Console** -> *Configuration* -> *System*".

Exchange Server can be setup either using the **Exchange Admin Centre Console** or Exchange Management PowerShell Command Prompt.

Note: Refer to the steps given under Appendix > Exchange Server setup using Exchange Management Shell – Quick Reference for more details.

5.1.1 Using Exchange Admin Centre Console

Steps for setting up exchange server using the Exchange Admin Centre Console are given below –

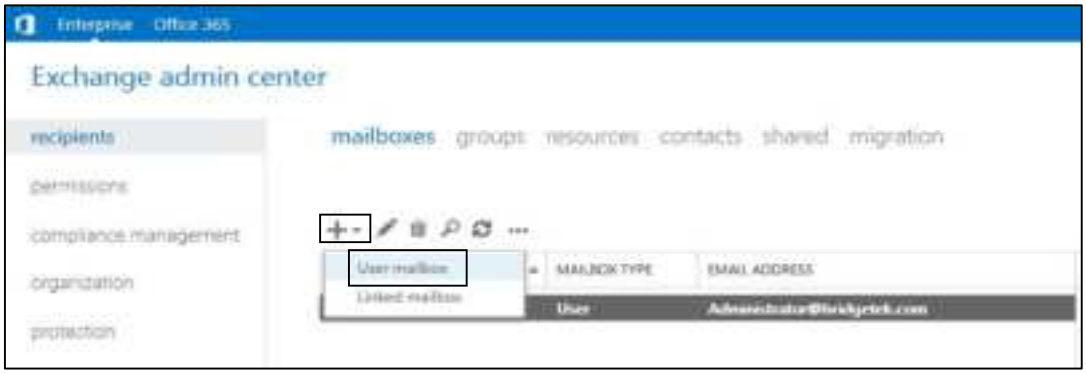
→ **Login to Exchange Admin Centre Console**

- Go to **https://<exchange servername>/ecp** and log in with Exchange Admin account.

→ **Create User Account**

- Go to **"recipients"** → **"mailboxes"**.

- Click **"+"** and select **"User mailbox"**.



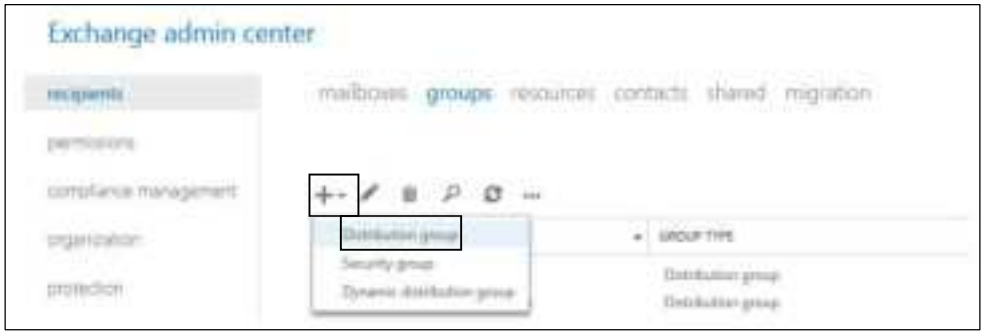
- Enter the user account details and click **[Save].**

- The newly created User account will be displayed under the list of mailboxes.

→ Create Distribution Group for Users

- Go to **"recipients" → "groups".**

- Click **"+"** and select **"Distribution group"**.



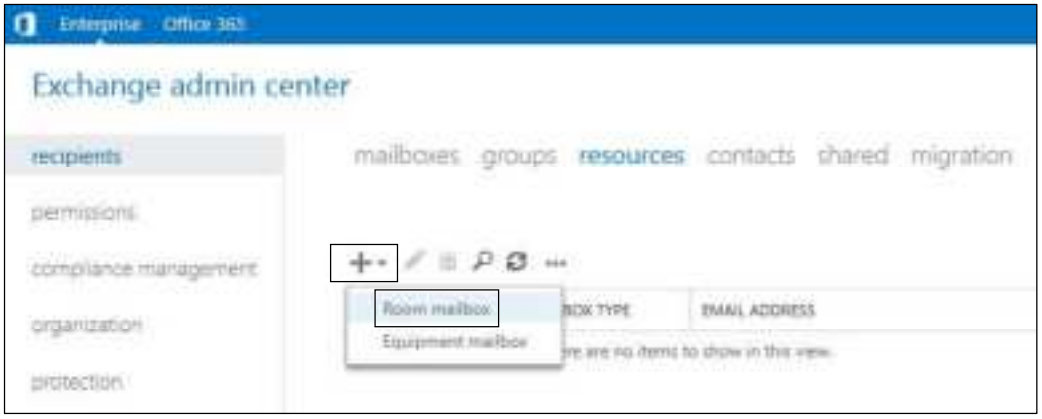
- Enter the new distribution group information and click **[Save]**.

- The newly added distribution group is displayed.

→ Create Desk / Resource Account

- In the Exchange admin centre go to **"recipients" → "resources"**.

- Click **"+"** and select **"Room mailbox"**.



- Enter the Desk account details and click **[Save].**

- The newly created desk account will be displayed under the list of resources.

→ Create Distribution Group for Desks

The distribution group for Desks (RoomList) can be created **only** using the PowerShell command.

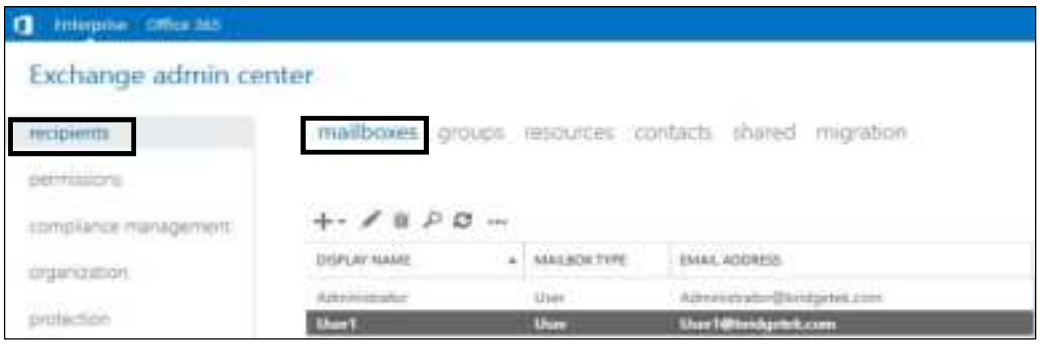
For example, the command to create a new user distribution group named *"pdm-user-group-<groupname>"* is -

```
New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList
```

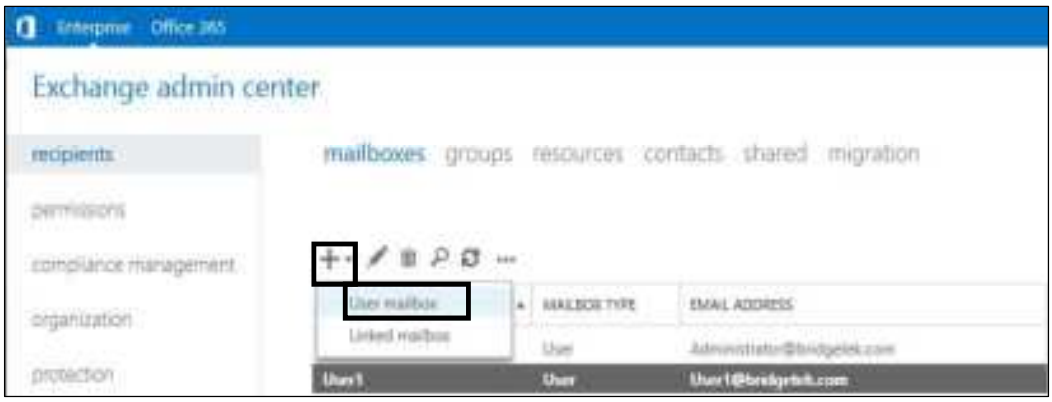
Note: A distribution group name should begin with prefix *pdm-desk-group* and be followed by the group name.

→ Create Impersonation User / Service Account

- Go to **"recipients"** → **"mailboxes"**.

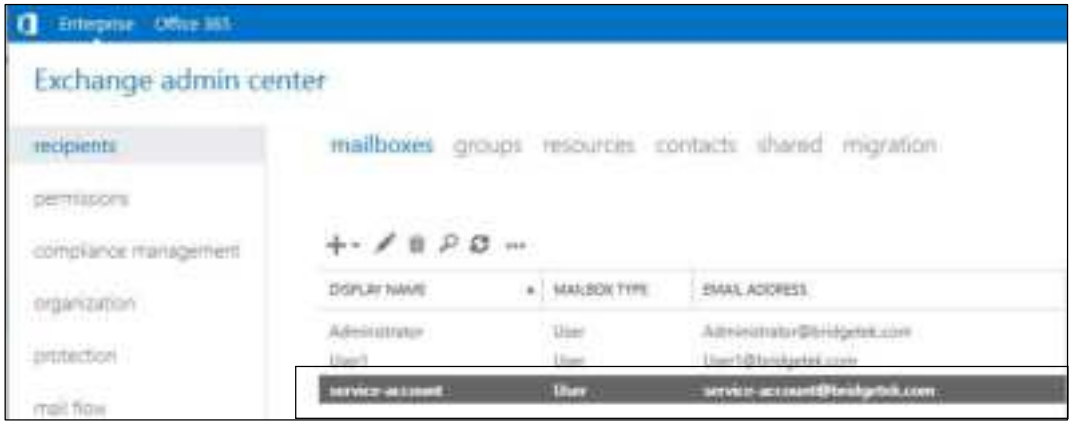


- Click **+** and select **User mailbox**.



- Enter the Service Account details and click **[Save].**

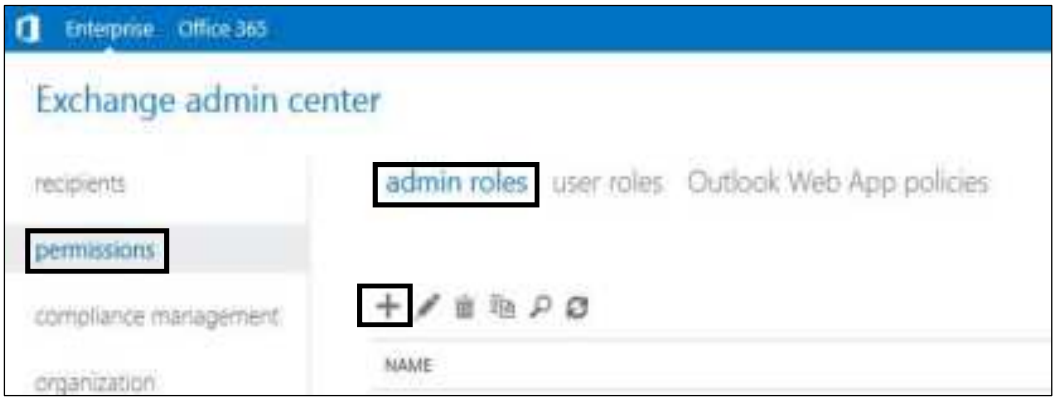
- The Service account will appear in the list of mailboxes.



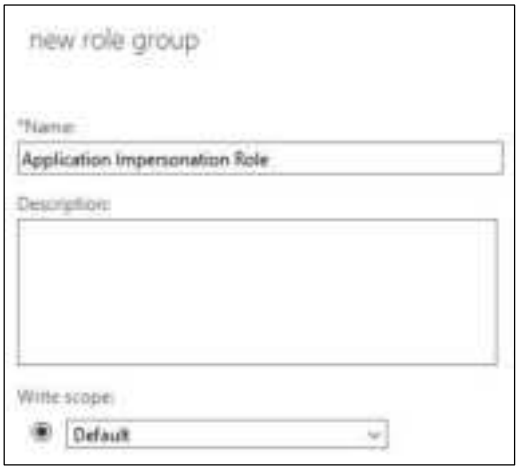
→ Granting Service Account Impersonation Rights

The following steps will guide to grant the service account with impersonation permission for **all accounts –**

- In the Exchange admin centre, navigate to **"permissions" → "admin roles"**. Click **"+"**.

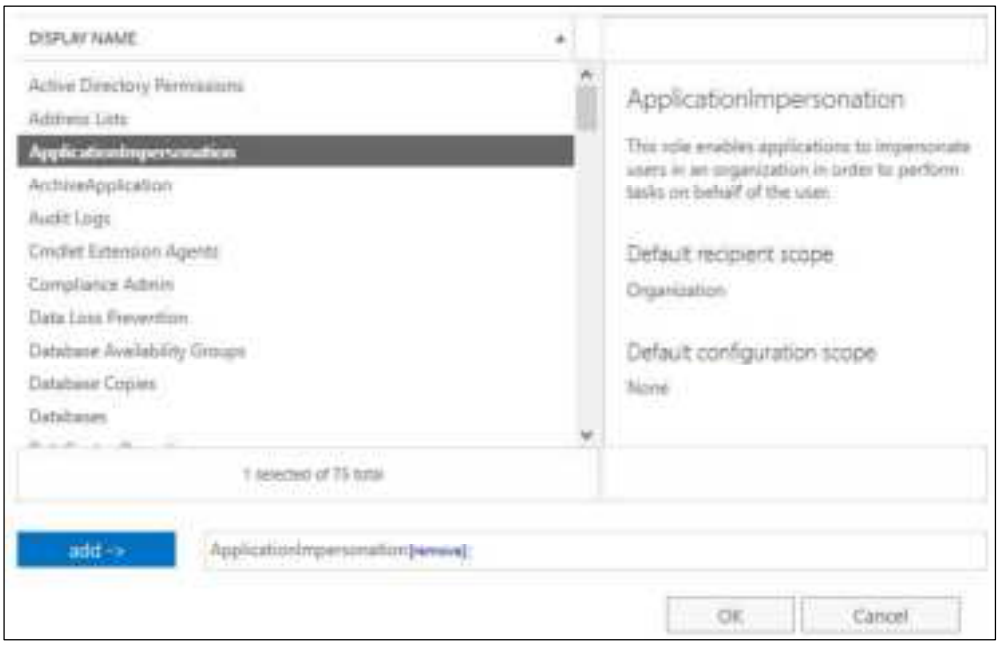


- Input the role group related details. Set the *"Write scope"* field as **Default** (for all accounts).



- Click **"+"** under **"Roles"**.

- Add the admin role **"ApplicationImpersonation"**. Click **[OK]**.



- The newly added admin role will be displayed under **"Roles"**.

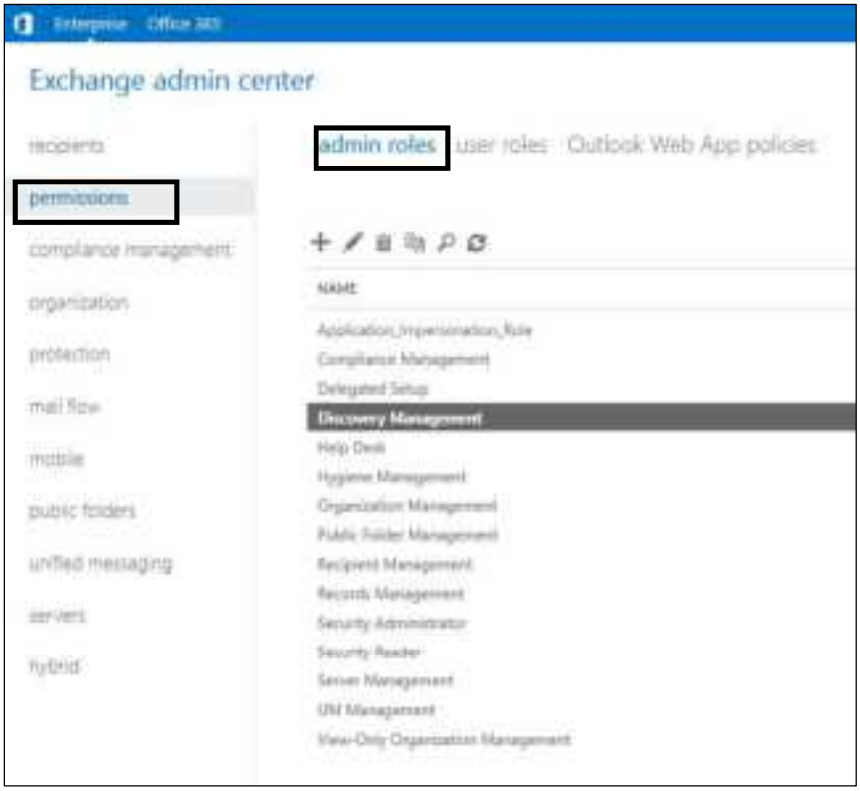
- Similarly, click **"+"** under **"Members"** and add the service account and click **[OK]**. Service account will be added and displayed. Click **[Save]**.

- The newly added role is displayed under the **"admin roles"**.

→ Discovery Management

Members of this management role group can perform mailbox search in the Exchange organization for data that meets specific criteria.

- In the Exchange admin centre, navigate to **"permissions" → "admin roles"**. Click and select **"Discovery Management"**.



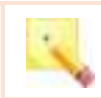
- In the **"Discovery Management"** interface, enter the Name, Under **Rules**, select *"Legal Hold"*; select the *"Service Account"* under **Members**.

- Similarly, click **"+"** under **"Members"** and add the service account and click **[OK]**. Service account will be added and displayed. Click **[Save]**.

5.2 Microsoft 365 Setup

Account Reference	Account Type	Number of Accounts	Description
User Account	User Mailbox	X	This account will be used by the normal end users to perform desk booking related activities.
Distribution Group for Users	Group (Users)	X	This group of users (**pdm-user-group-**<groupname>) are only allowed to access the following PDM components – • PDM Management Console • Outlook Add Ins • PanL PD35L device On spot booking
Resource Account	Desk Mailbox	X	These are accounts associated with the desk resource. • This account will be part of the distribution group.
Distribution Group for Desks	Group (Room List)	X	This group of desks (**pdm-desk-group-**<groupname>) are only allowed to access the following PDM components – • PDM Management Console • Outlook Add Ins • PanL PD35L device On spot booking
Impersonation User / Service Account	User	1	This user will be able to access multiple mailboxes and act as the mailbox owner. This account will be used – • To communicate between PDM and Exchange Server. • All the PDM Server / Desk Booking related emails will be sent by this user • Upon installation of PDM Server, this user account details must be added in the "**PDM Management Console** -> *Configuration* -> *System*".

Microsoft 365 can be setup either using the **Microsoft 365 Admin Centre Console** or Windows PowerShell Command Prompt.



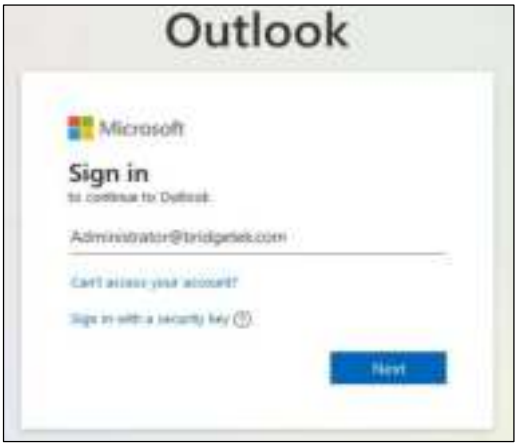
Note: Refer to the steps given under Appendix > Microsoft 365 setup using Windows Powershell – Quick Reference for more details.

5.2.1 Using Microsoft 365 Admin Center Console

Steps for setting up exchange server using the Exchange Admin Center Console are given below –

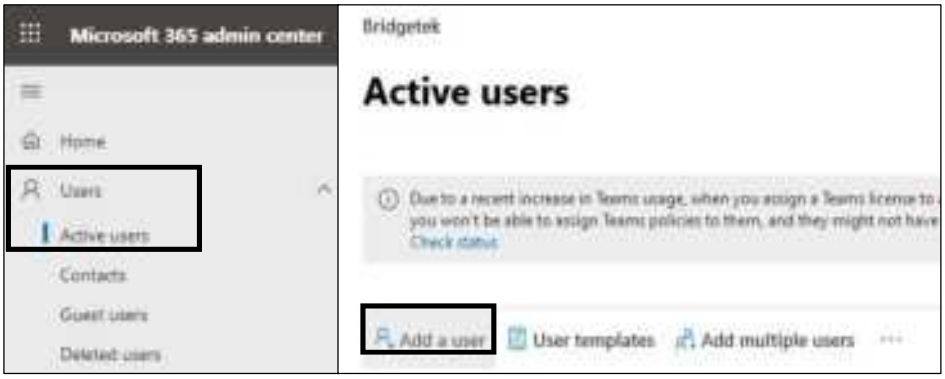
→ **Login to Microsoft 365 Admin Center Console**

- Go to the Microsoft 365 Admin center and log in with Microsoft 365 admin account.



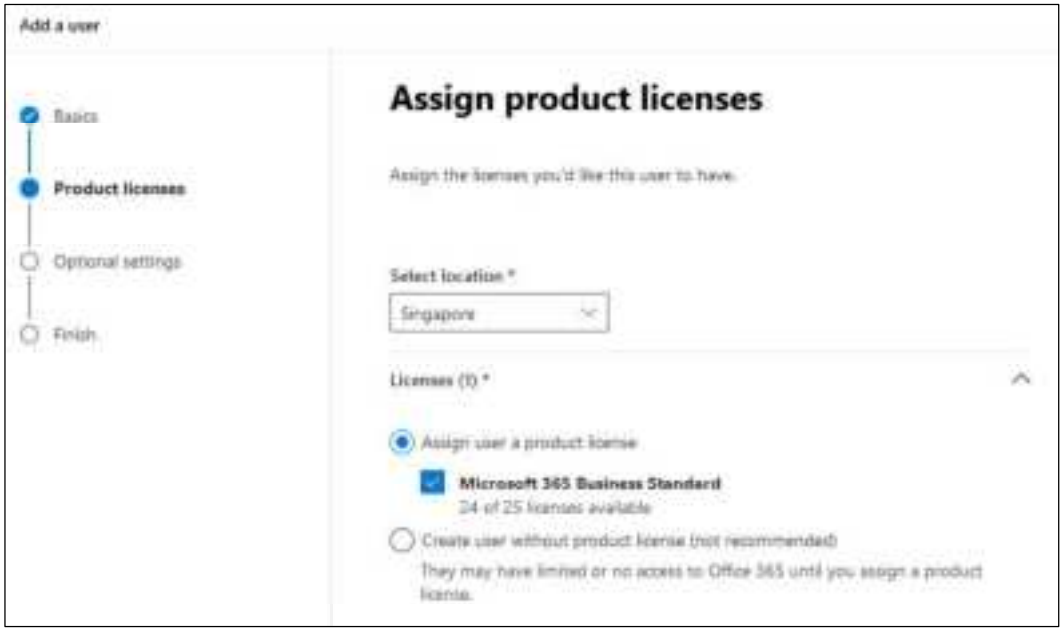
→ **Create User Account**

- In the Microsoft 365 admin centre, click **"Users → Active Users → Add a user"**.

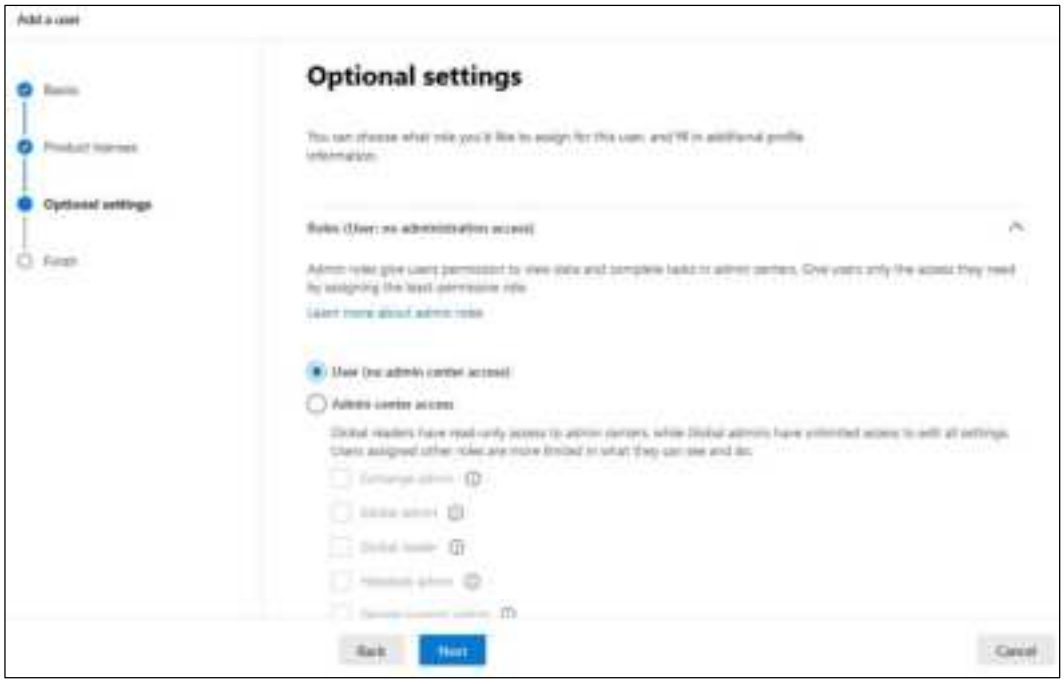


- Enter the basic information pertaining to User account. Click **[Next]**.

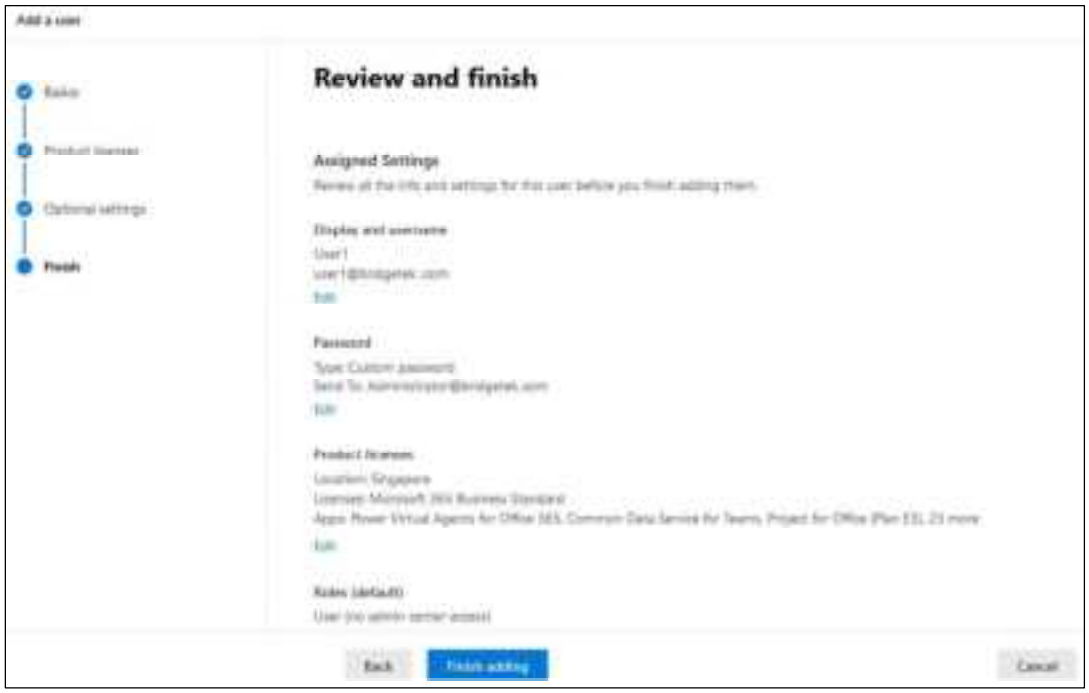
- Assign the **"product licenses"**. Click **[Next]**.

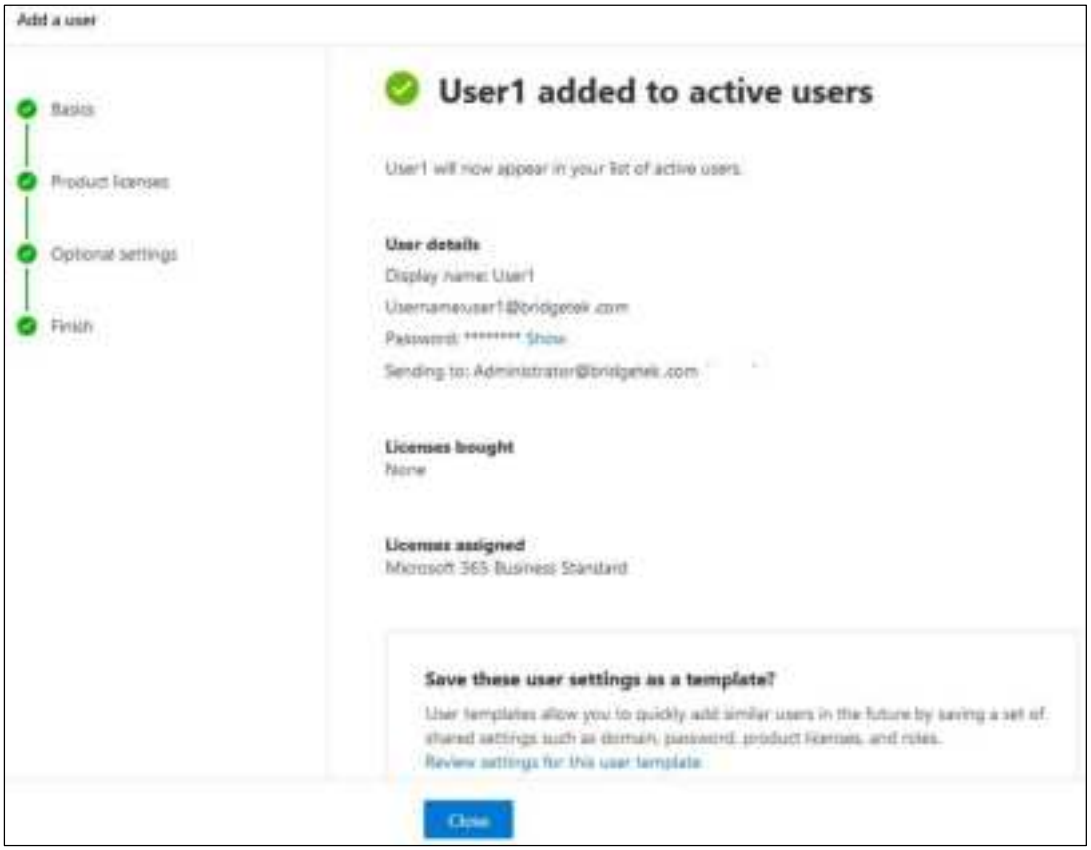


- Go through the **Optional settings** and select as required. Click **[Next]**.

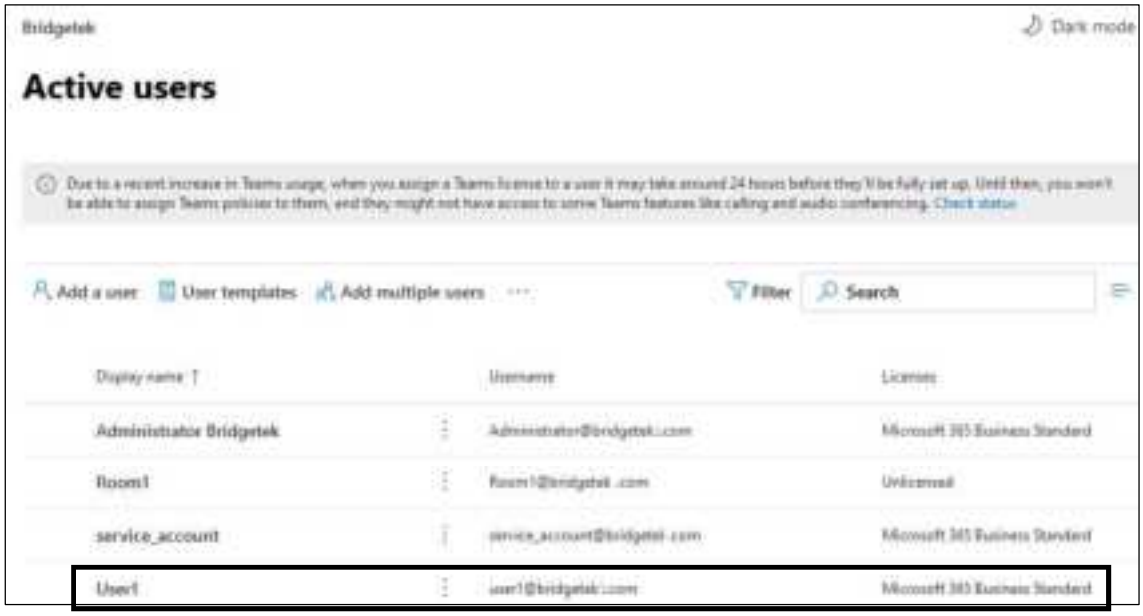


- Verify the user account details and click **[Finish Adding]**.



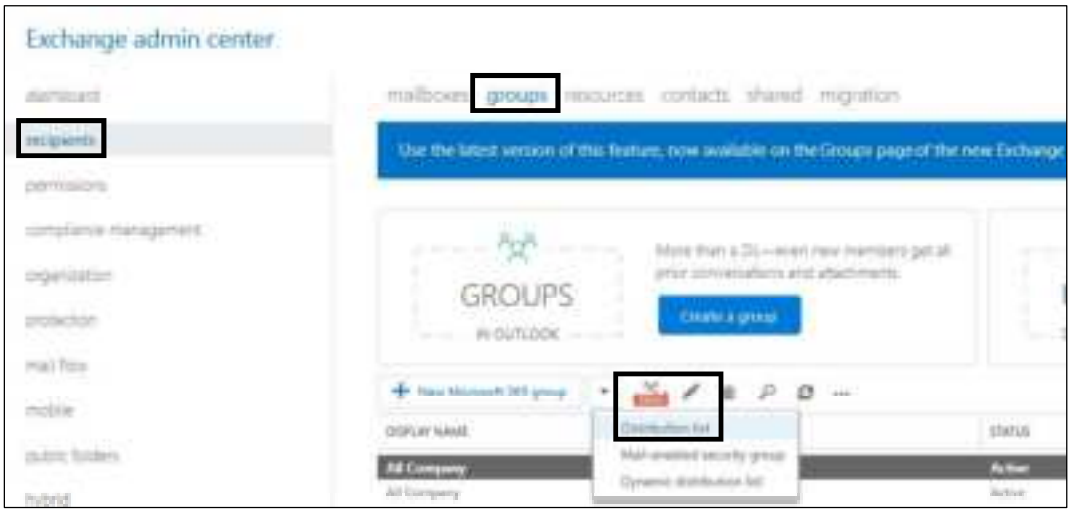


The user account details are added to active users list.

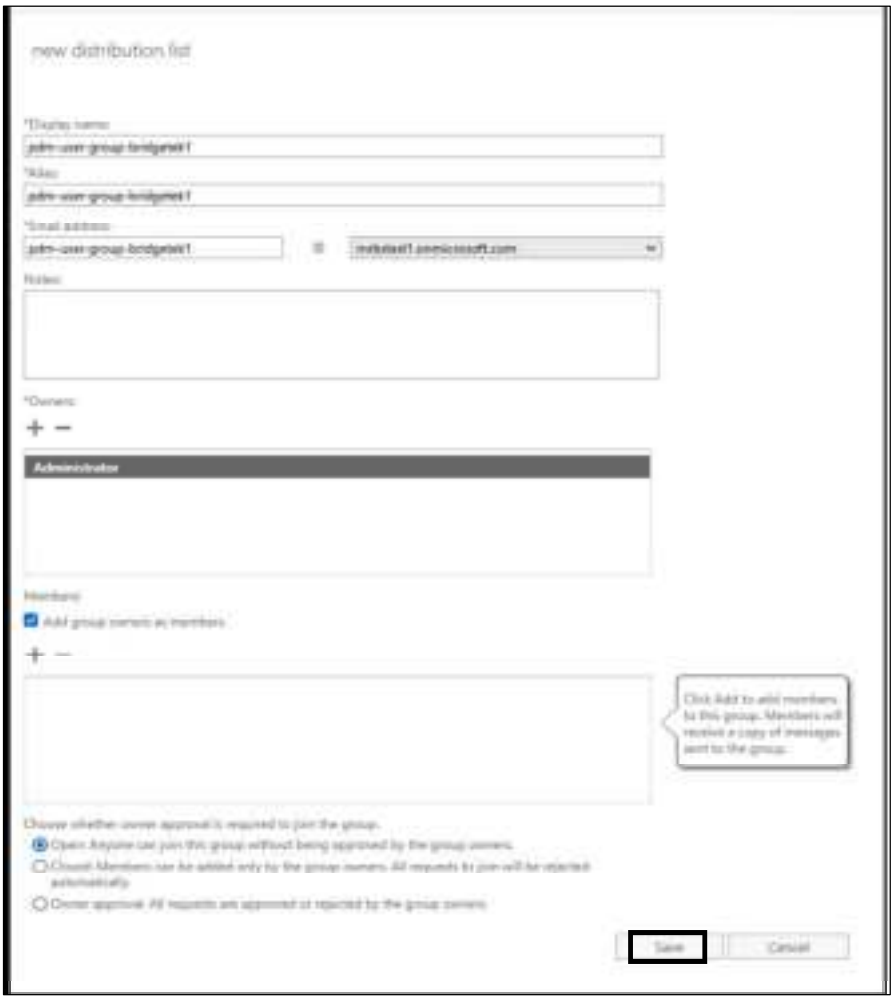


→ Create Distribution Group for Users

- Go to **"recipients"** → **"groups".** Click **"new"** and select **"Distribution list"**.



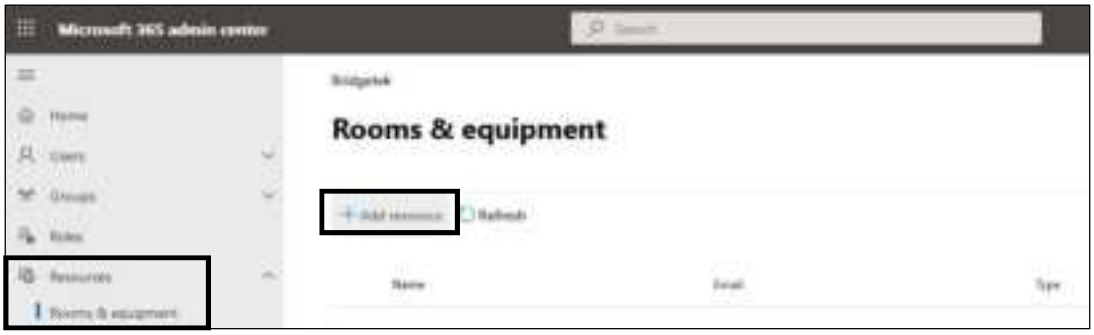
- Enter the new distribution list related information and click **[Save]**.



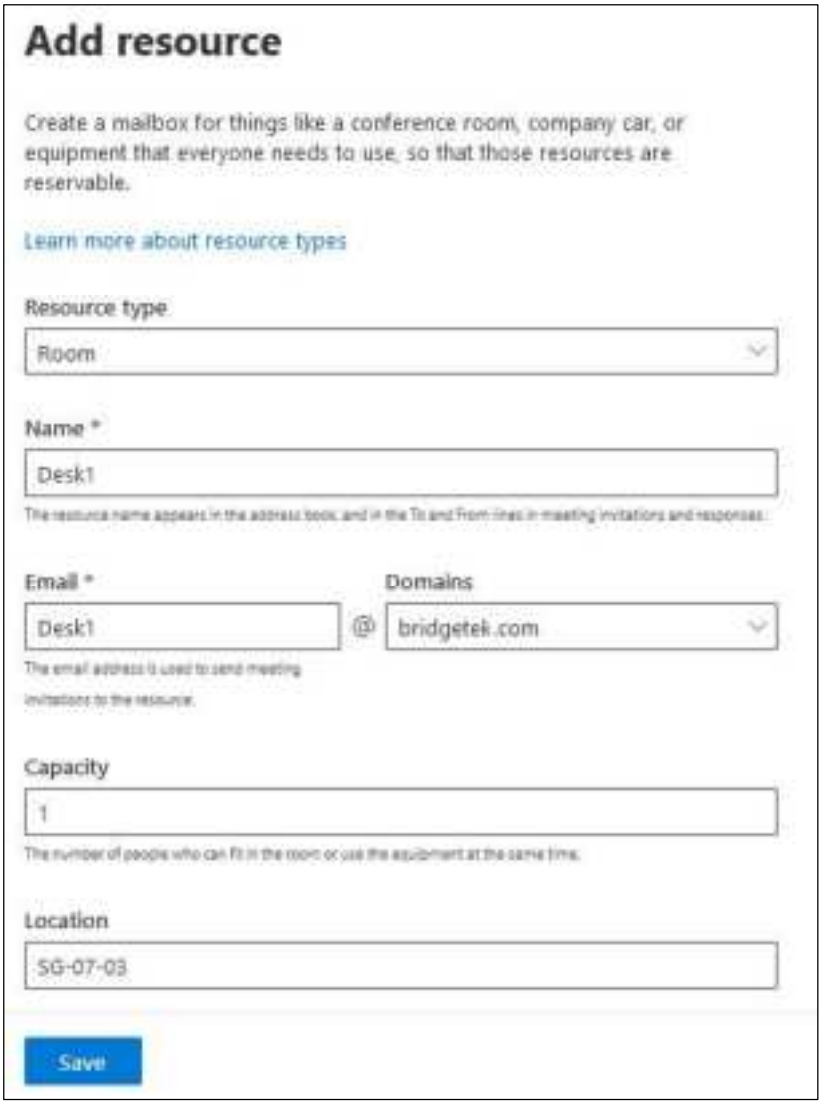
- The newly added distribution list is displayed.

→ Create Desk / Resource Account

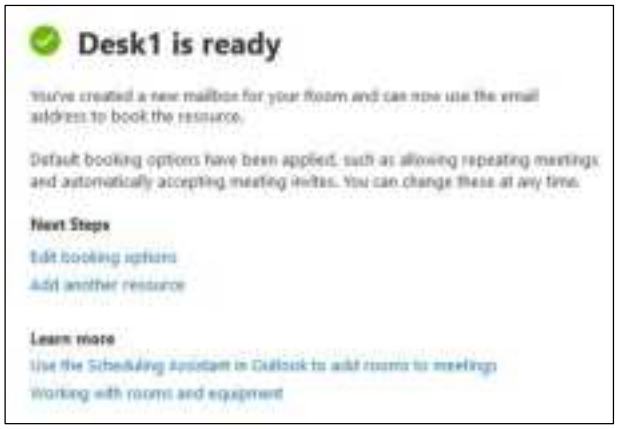
- Go to **"Resources"** → **"Rooms & equipment".** Click **"+Add resource"**.

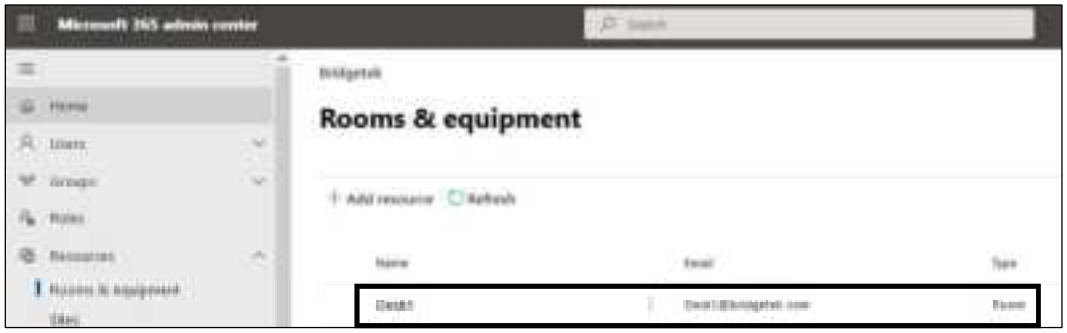


- In the **Add resource** interface, enter the following resource related information **–** *Resource Type, Resource Name, Email address, Capacity & Phone number*. Click **[Save]**.



- A new resource (desk) account is added and displayed.



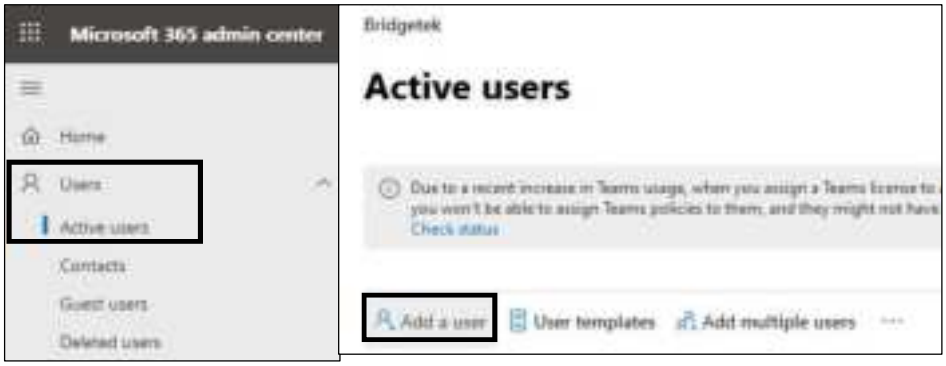


→ Create Distribution Group for Desks

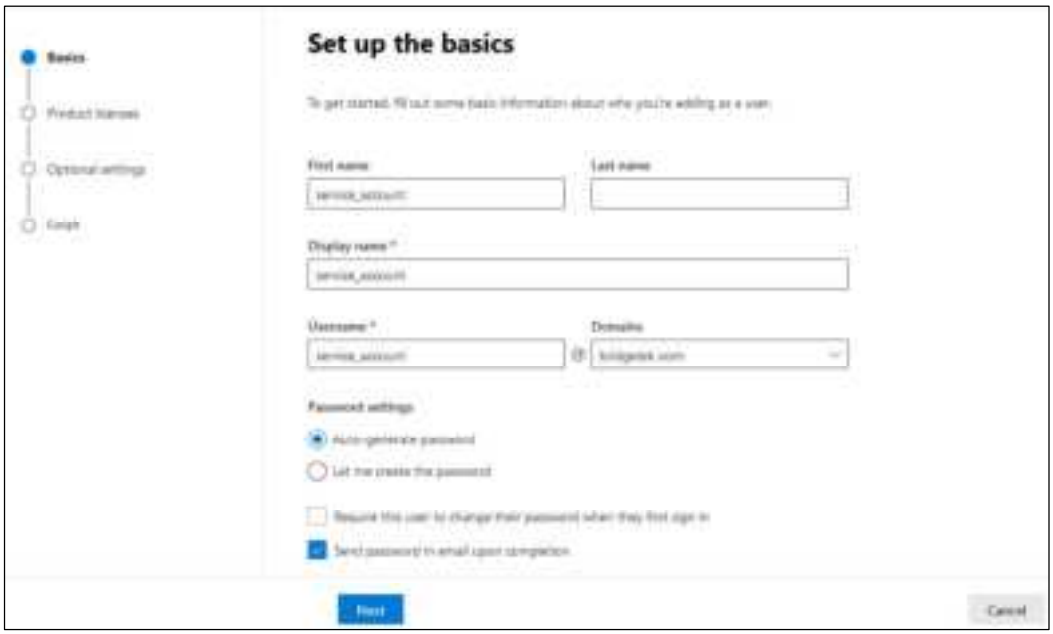
The distribution group for Rooms (RoomList) can be created **only** using the Exchange PowerShell.

→ Create Impersonation User / Service Account

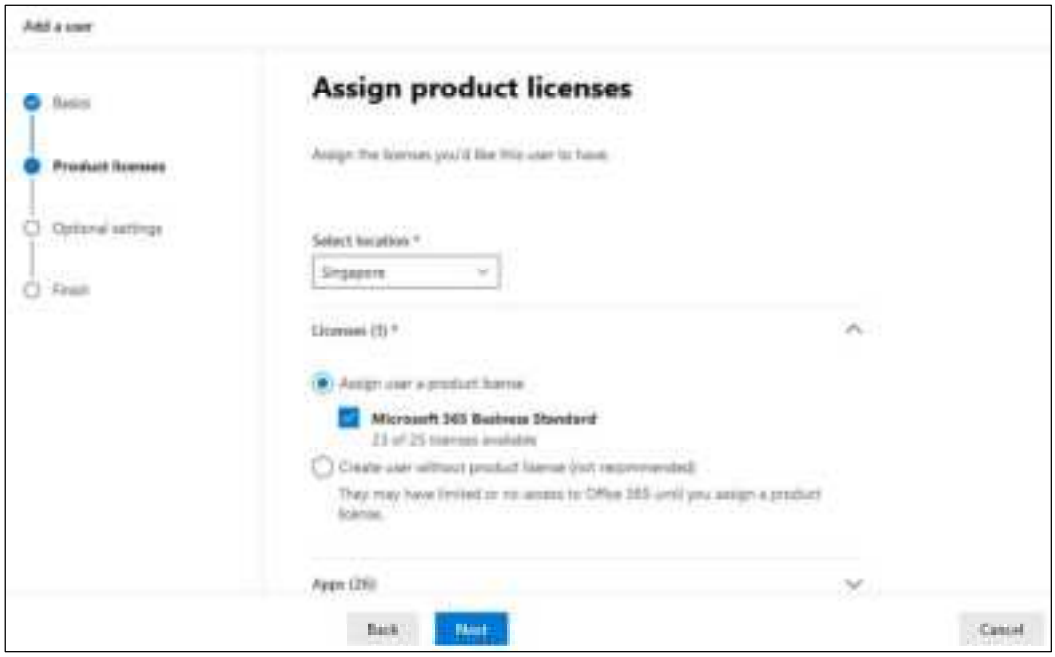
- In the Microsoft 365 admin centre, click **"Users → Active Users → Add a user"**.



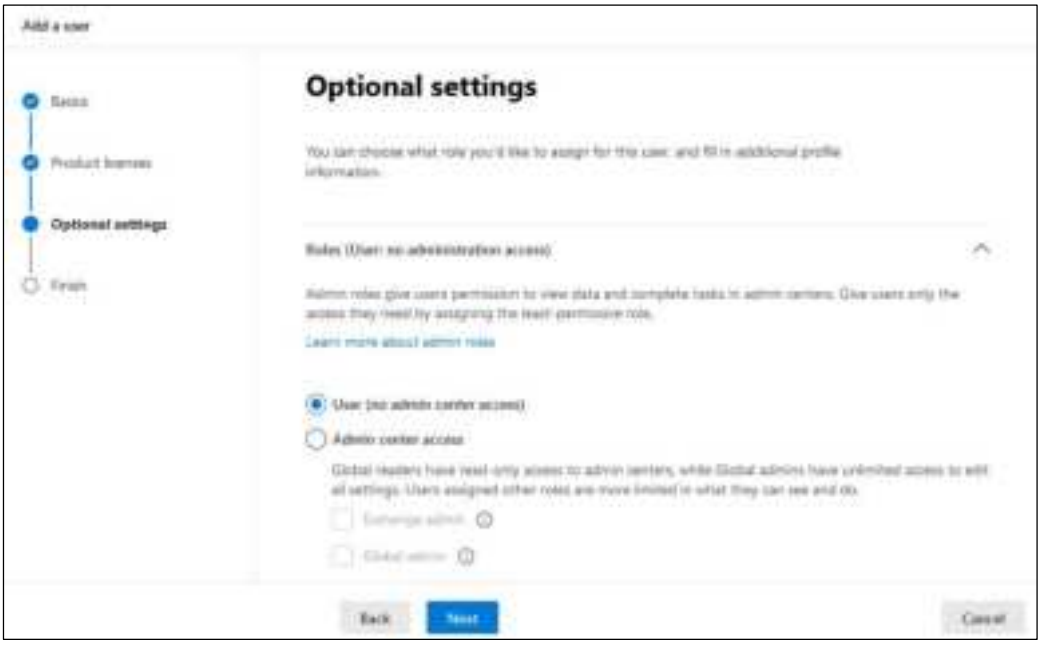
- Enter the basic information pertaining to Service Account. Click **[Next]**.



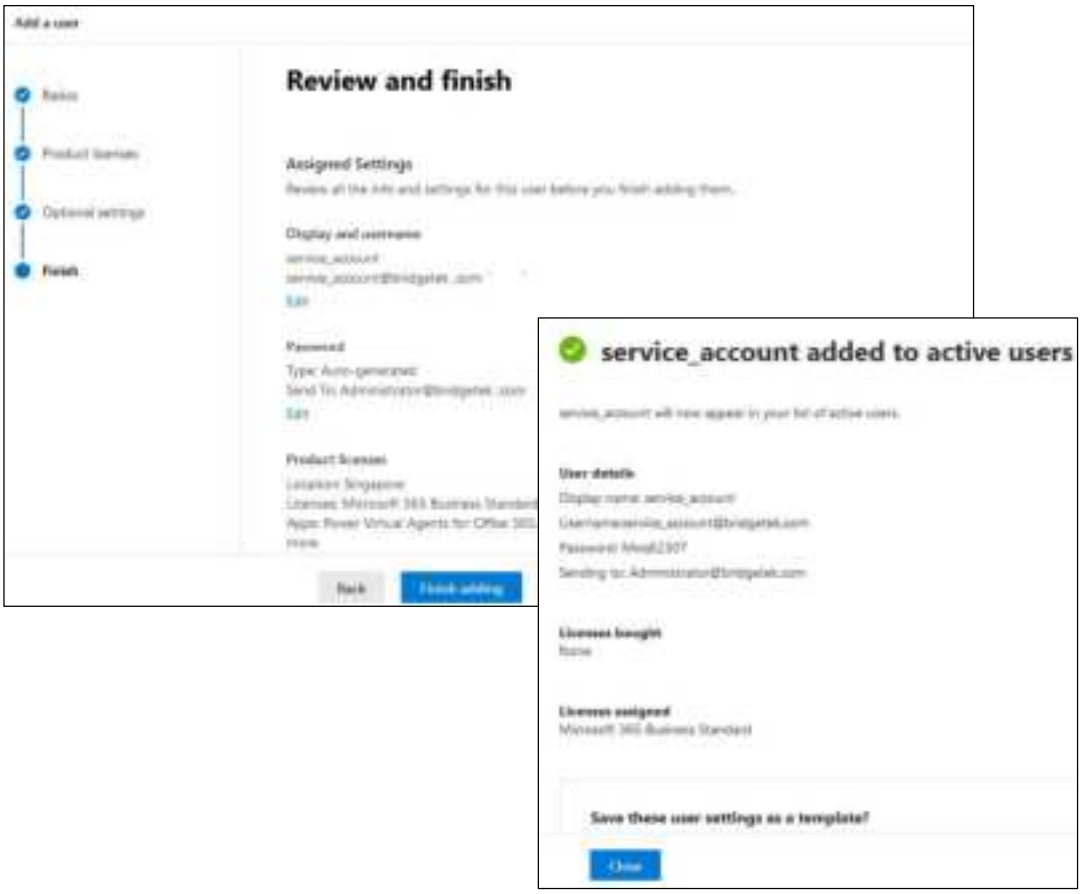
- Assign the **"product licenses"**. Click **[Next]**.



- Go through the **Optional settings** and select as required. Click **[Next]**.



- Verify the details and click **[Finish Adding]**.



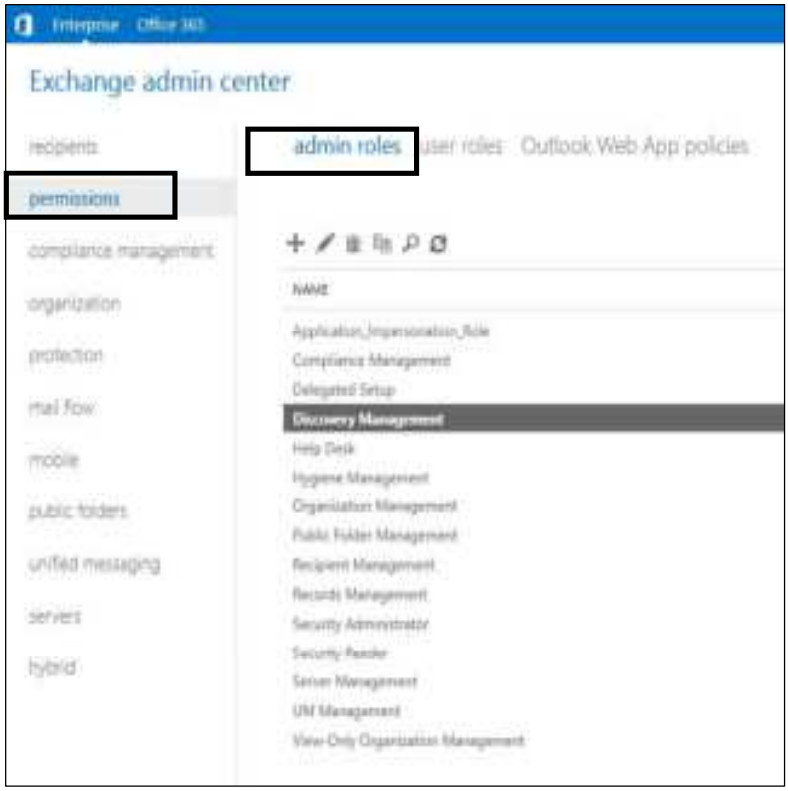
- The service account details are added to active users list.

→ Granting Service Account Impersonation Rights

Refer to the steps given under section Granting Service Account Impersonation Rights in Exchange.

→ Discovery Management

- In the Microsoft 365 admin centre, navigate to **"permissions" → "admin roles"**. Click and select **"Discovery Management"**.



- In the **"Discovery Management"** interface, enter the Name, Under **Rules**, select *"Legal Hold"*; select the *"Service Account"* under **Members**.

- Similarly, click **"+"** under **"Members"** and add the service account and click **[OK]**. Service account will be added and displayed. Click **[Save]**.

5.2.2 Modern Authentication using OAuth 2.0 – Open ID-Connect (OIDC)

→ Access Azure Portal using the administrator account - https://portal.azure.com

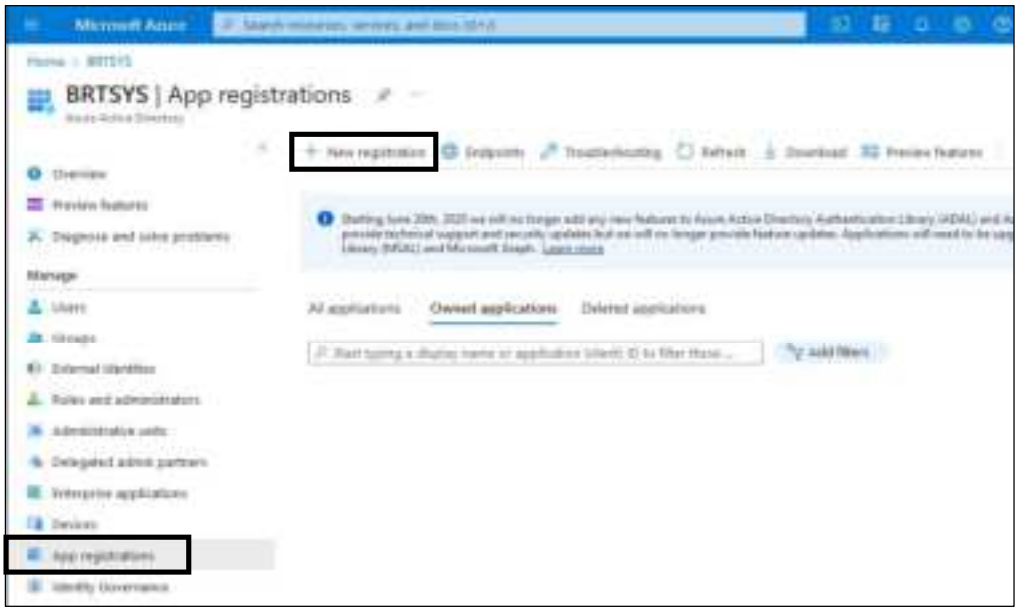
→ Go to **Azure Active Directory** from the left navigation menu.

- Register Applications
- Setup Authentication (Redirect URI)
- Setup Client Secret
- Setup API Permissions

5.2.2.1 PDM Client

5.2.2.1.1 App Registration

→ Select **App registrations**. Click **+ New registration**.



→ Enter the ***Application name –*** *PDM Client*; select the ***Supported account types –*** *Accounts in this organisation directly only* from the available options. and click **[Register]**.

→ The PDM Client application is successfully created.

5.2.2.1.2 Setup Authentication (Redirect URI)

→ Go to ***Authentication page*** and click on ***+ Add a platform***. Select **Web**.

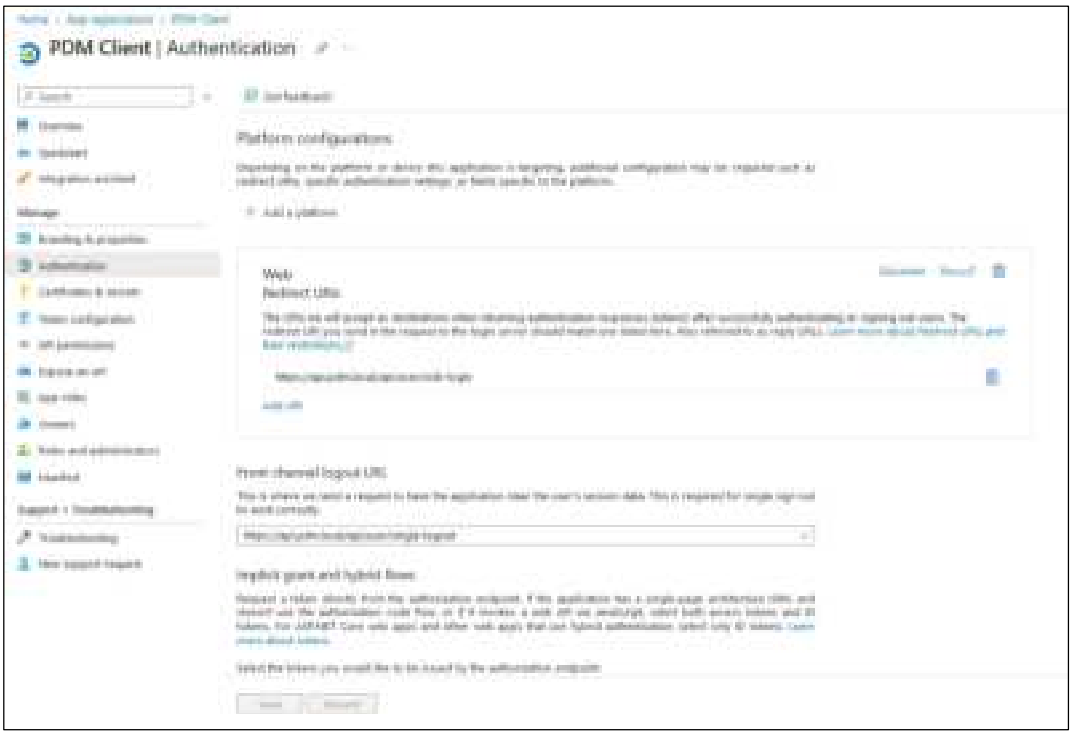
→ In the configure Web UI –

- (Optional) Enter the **Redirect URIs** - *https://api.pdm.local/api/user/oidc-login*
- Enter the **Front-channel logout URL –** PDM Front-channel Logout URI (*https://api.pdm.local/api/user/single-logout*). This field is needed only when implementing single sign on. **(Mandatory)**.

  pdm.local - indicates the domain name.

- Select ***ID tokens*** check box
- Click **[Configure]**.

→ The configuration details are displayed.



5.2.2.1.3 Setup Client Secret

→ In the left menu, select **Certificates & secrets**; click **+ New client secret**.

→ In the **Add a client secret UI**, enter the *Description*; choose an *expiration period* and click **[Add]**.

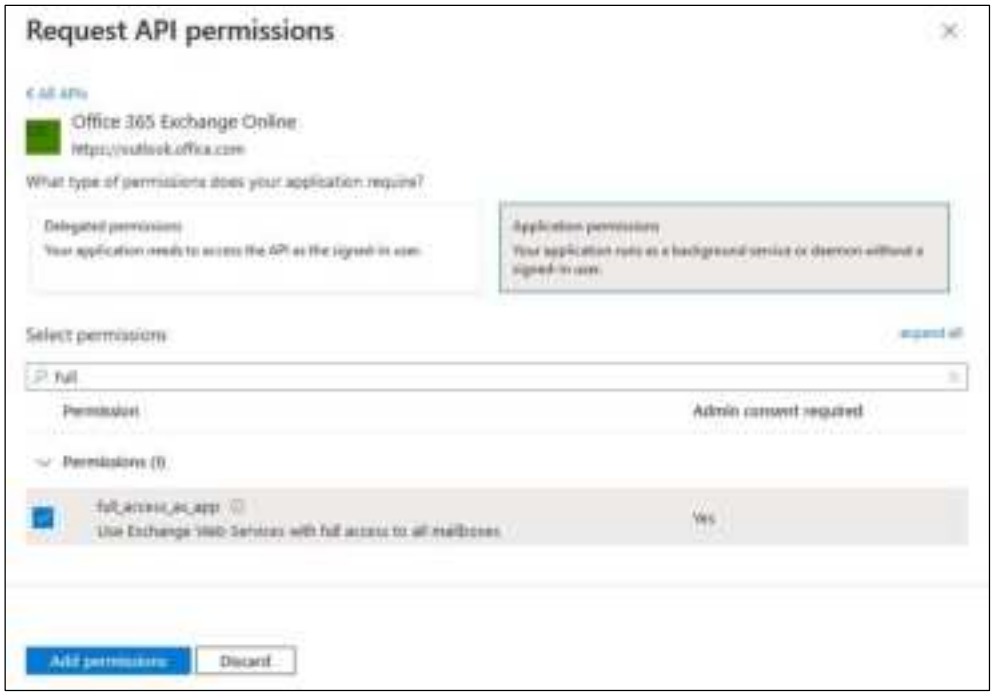
→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.

5.2.2.1.4 Setup API Permissions

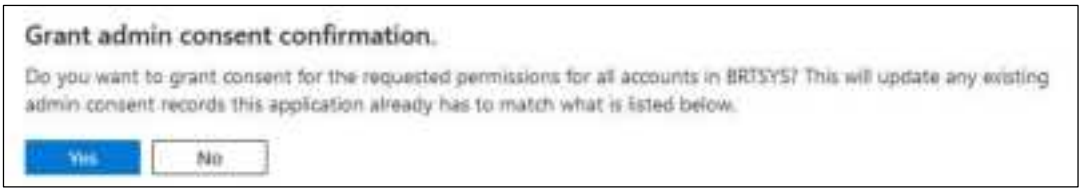
→ From left navigation menu, go to ***API permissions*** → + ***Add a permission***.

→ Go to the ***APIs my organization uses*** tab, type ***Office 365*** in the search bar; Click and select **Office 365 Exchange Online** from the search result.

→ Click ***Application permissions***; Check ***full_access_as_app***; Click ***Add permissions***.



→ The Office365 administrator must grant the permissions to be added. Click ***Grant admin consent for BRTSYS***. Click **[Yes]** to confirm.

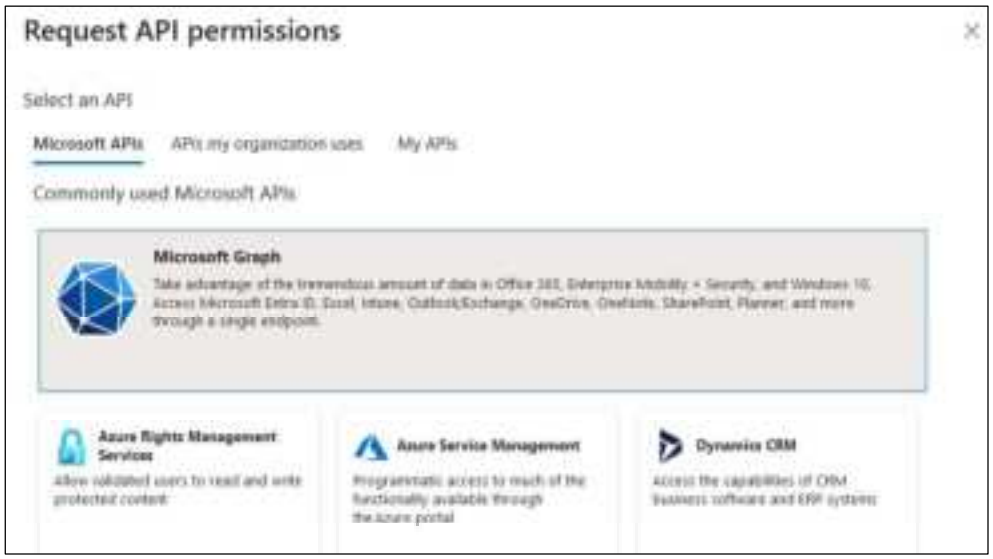


→ Upon successfully granting permission, a green check mark will appear.

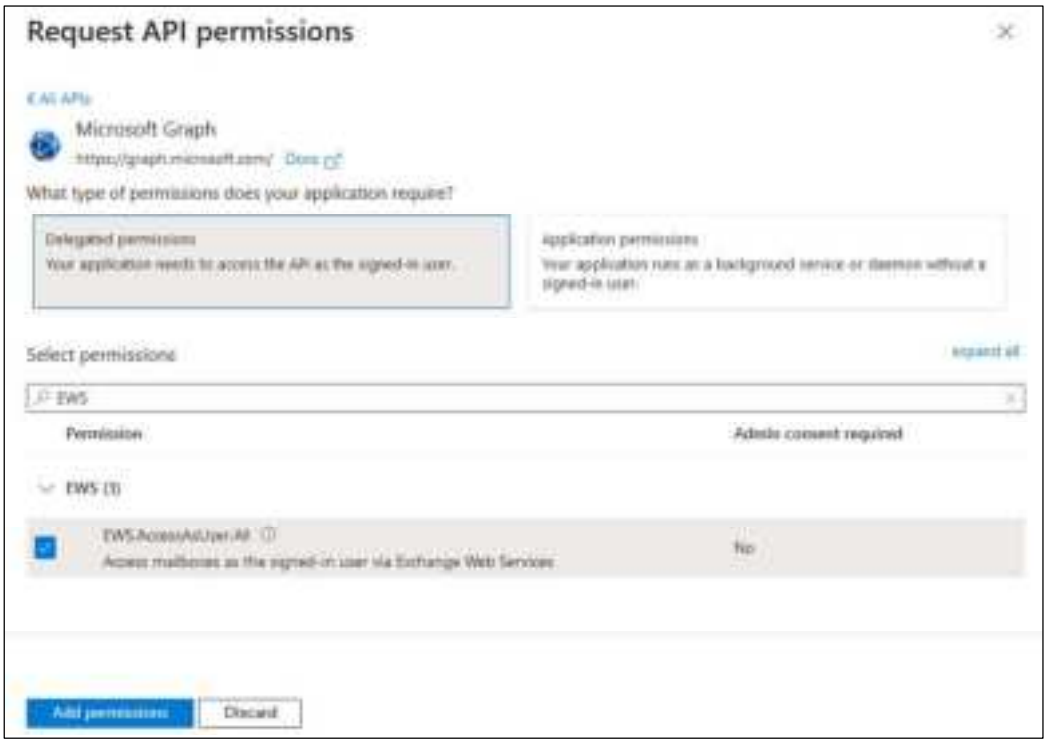
5.2.2.1.5 Setup Delegate Permissions

→ From left navigation menu, go to ***API permissions*** → + ***Add a permission***.

→ From the Request API permissions UI, click ***Microsoft APIs*** and select ***Microsoft Graph***.

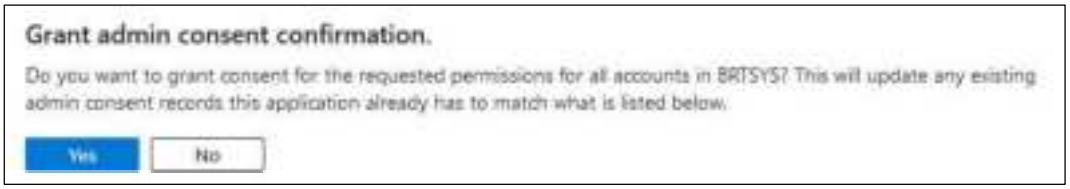


→ Select ***Delegated permissions***; ***Select permissions – EWS*** *(EWS.AccessAsUser.All)*. Click **[Add permissions]**.

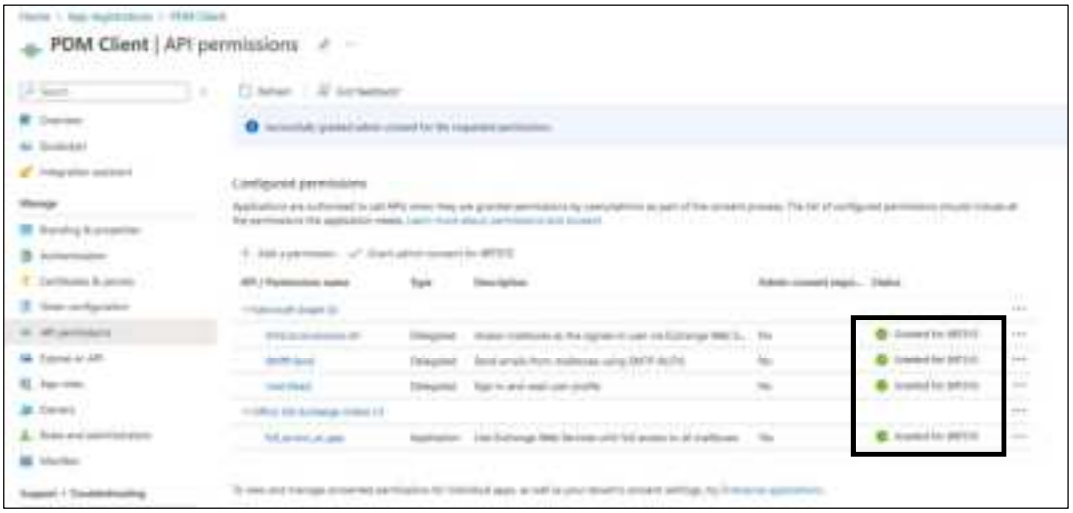


→ Select ***Delegated permissions***; ***Select permissions – SMTP*** (*SMTP.Send*). Click **[Add permissions]**.

→ The Office365 administrator must grant the permissions to be added. Click ***Grant admin consent for BRTSYS***. Click **[Yes]** to confirm.



→ Upon successfully granting permission, a green check mark will appear.

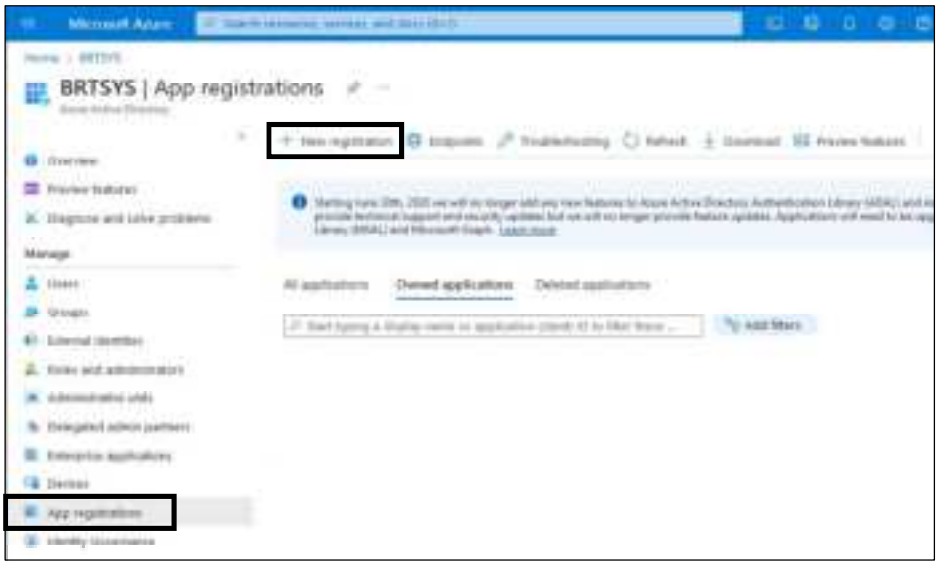


Note: More platforms and URIs for each platform can be added, depending on the need.

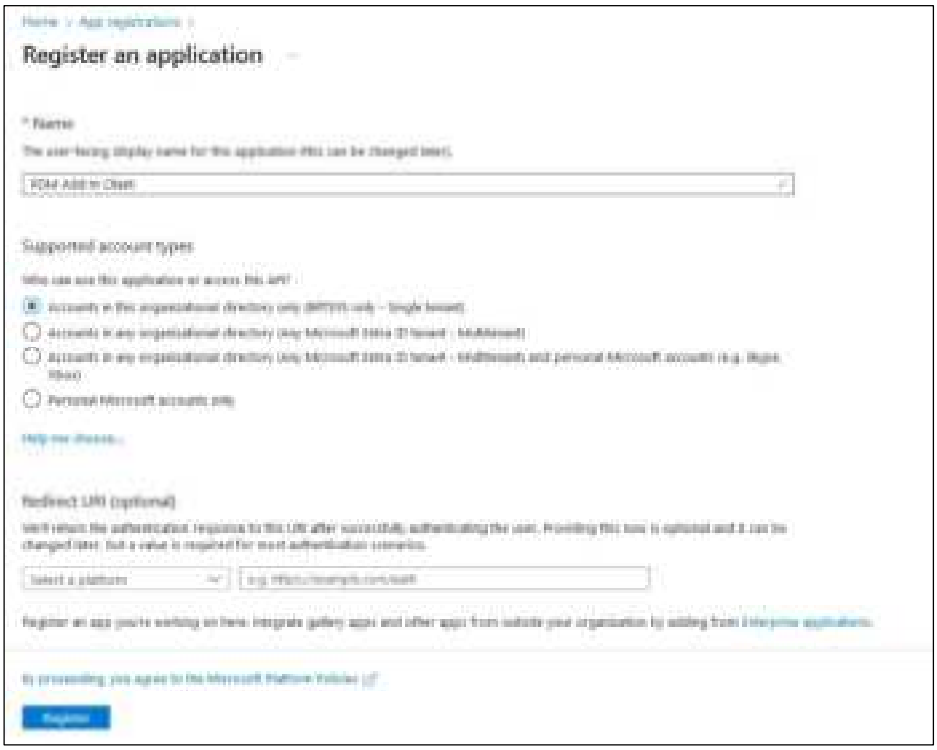
5.2.2.2 Add-In Client

5.2.2.2.1 App Registration

→ Select **App registrations**. Click **+ New registration**.



→ Enter the ***Application name*** **–** *PDM Add-In Client*; select the ***Supported account types*** **–** *Accounts in this organization directly only* from the available options. and click **[Register]**.



→ The PDM Add-In Client application is successfully created.

5.2.2.2.2 Setup Authentication (Redirect URI)

→ Go to ***Authentication page*** and click on ***+ Add a platform***. Select **Web**.

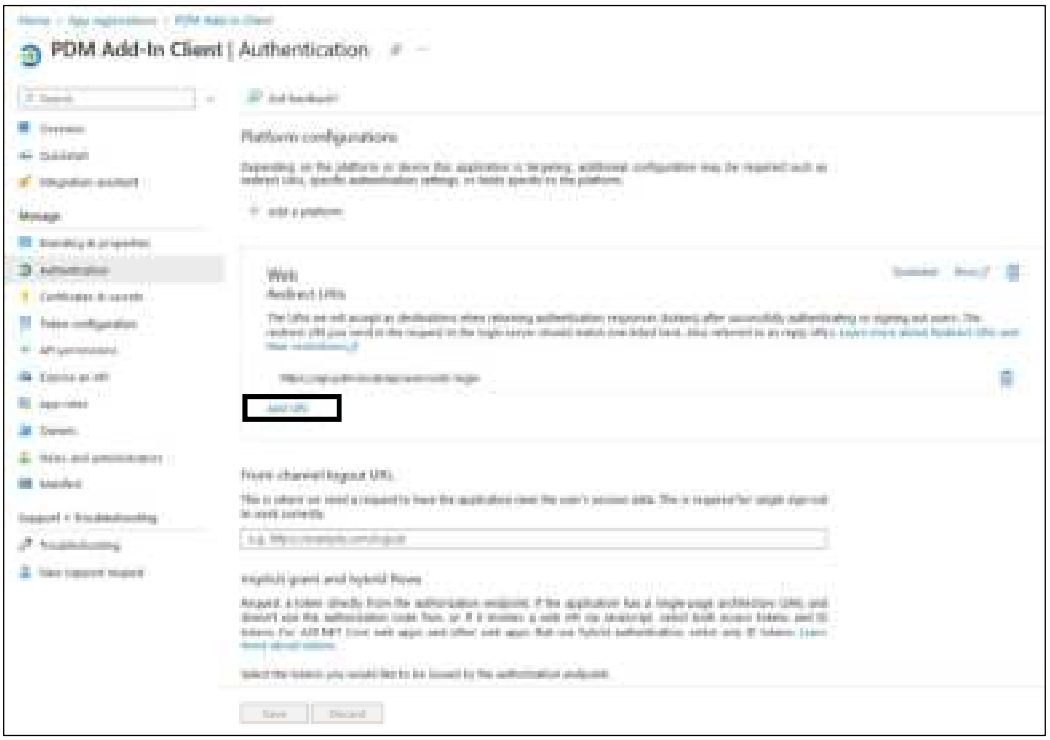
→ In the configure Web UI –

- Enter the **Redirect URIs –** PDM Login Redirect URI **–** For example, *https://api.pdm.local/api/user/oidc-login* **(Mandatory).**
- Enter the **Front-channel logout URL** - *https://api.pdm.local/api/user/single-logout*. This field is needed only when implementing single sign on. (Optional).

  pdm.local - indicates the domain name.

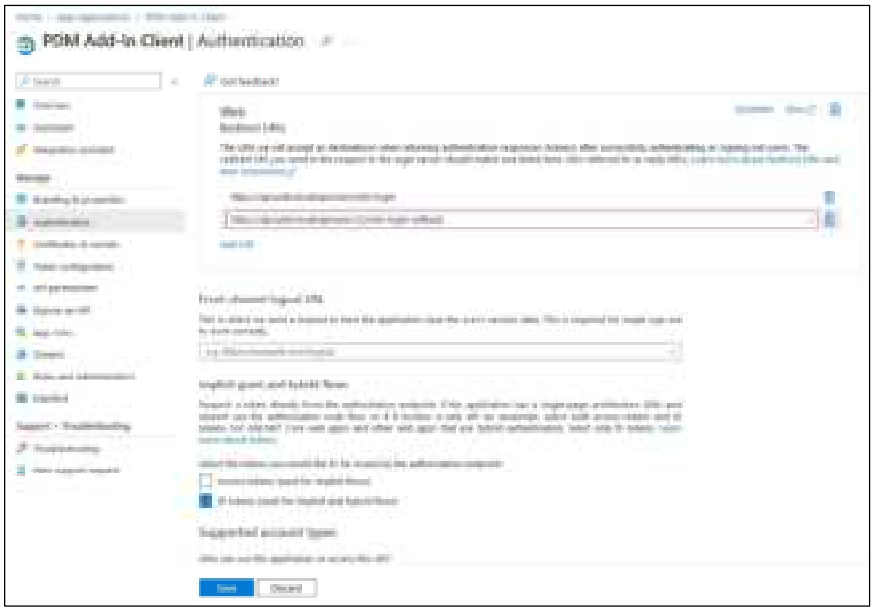
- Select ***ID tokens*** check box
- Click **[Configure]**.

→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



→ Enter the following details -

- **Redirect URIs –** PDM Login Redirect URI V2 **–** For example *https://api.pdm.local/api/user/v2/oidc-login-callback* **(Mandatory).** The highlighted text indicates the domain name.
- *Front-channel logout URL*. (Optional).
- Select ***ID tokens*** check box



→ Upon adding the redirect URIs, click **[Save]**.

5.2.2.2.3 Setup Client Secret

→ In the left menu, select **Certificates & secrets**; click **+ New client secret**.

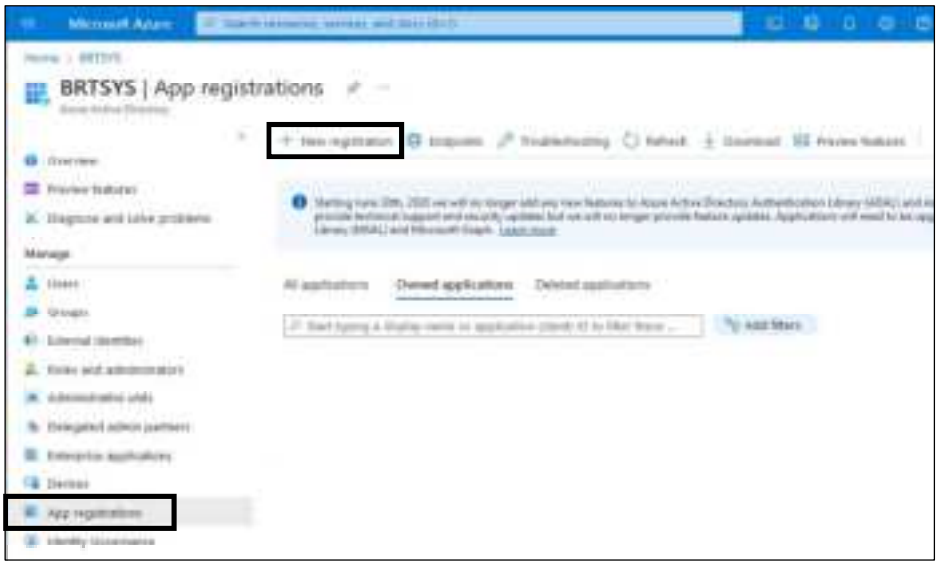
→ In the **Add a client secret UI**, enter the *Description*; choose an *expiration period* and click **[Add]**.

→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.

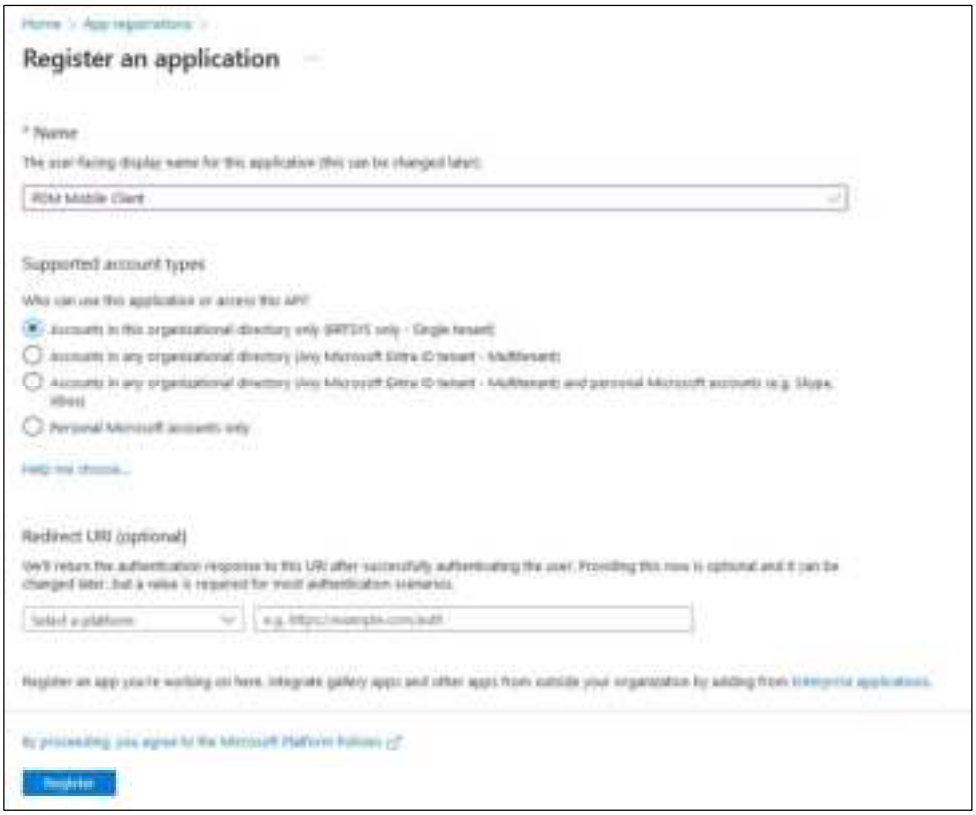
5.2.2.3 Mobile Client

5.2.2.3.1 App Registration

→ Select **App registrations**. Click **+ New registration**.



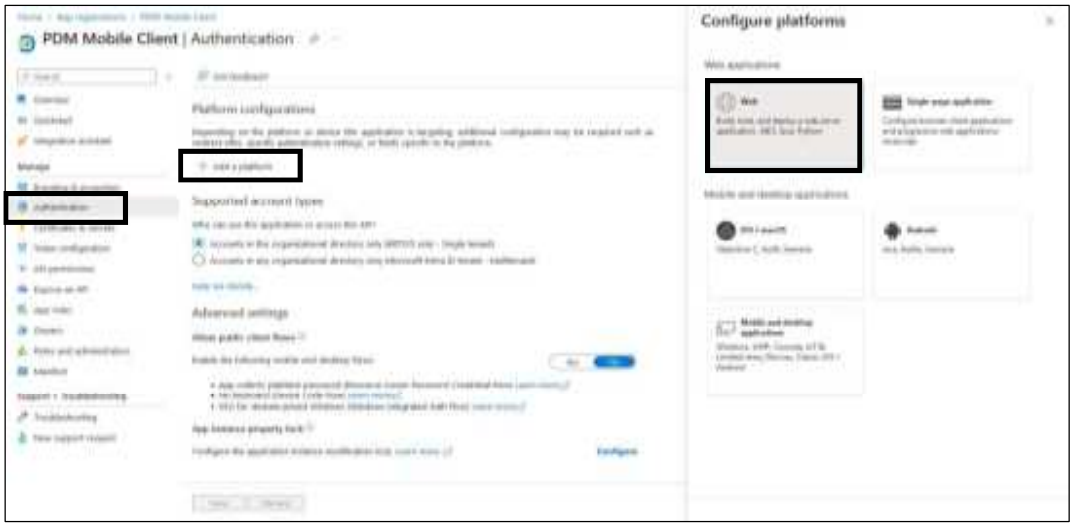
→ Enter the ***Application name*** **–** *PDM Add-In Client*; select the ***Supported account types*** **–** *Accounts in this organisation directly only* from the available options. and click **[Register]**.



→ The PDM Mobile Client application is successfully created.

5.2.2.3.2 Setup Authentication (Redirect URI)

→ Go to ***Authentication page*** and click on ***+ Add a platform***. Select **Web**.



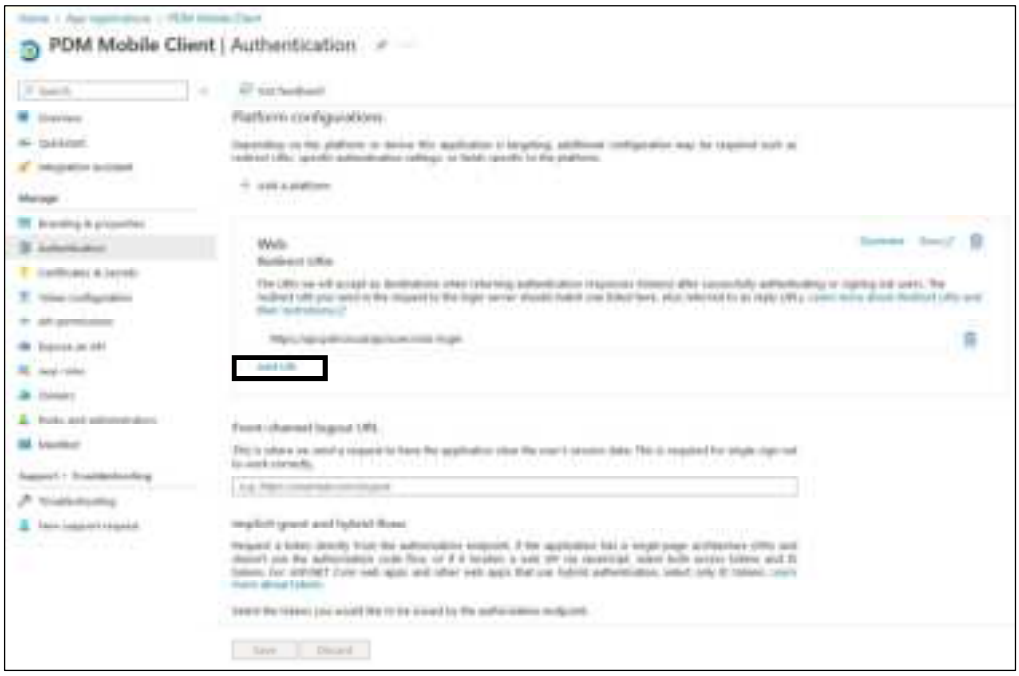
→ In the configure Web UI –

- Enter the **Redirect URIs** - PDM Login Redirect URI- For example, *https://api.pdm.local/api/user/oidc-login* **(Mandatory).**
- Enter the **Front-channel logout URL** - *https://api.pdm.local/api/user/single-logout*. This field is needed only when implementing single sign on. (Optional).

  pdm.local - indicates the domain name.

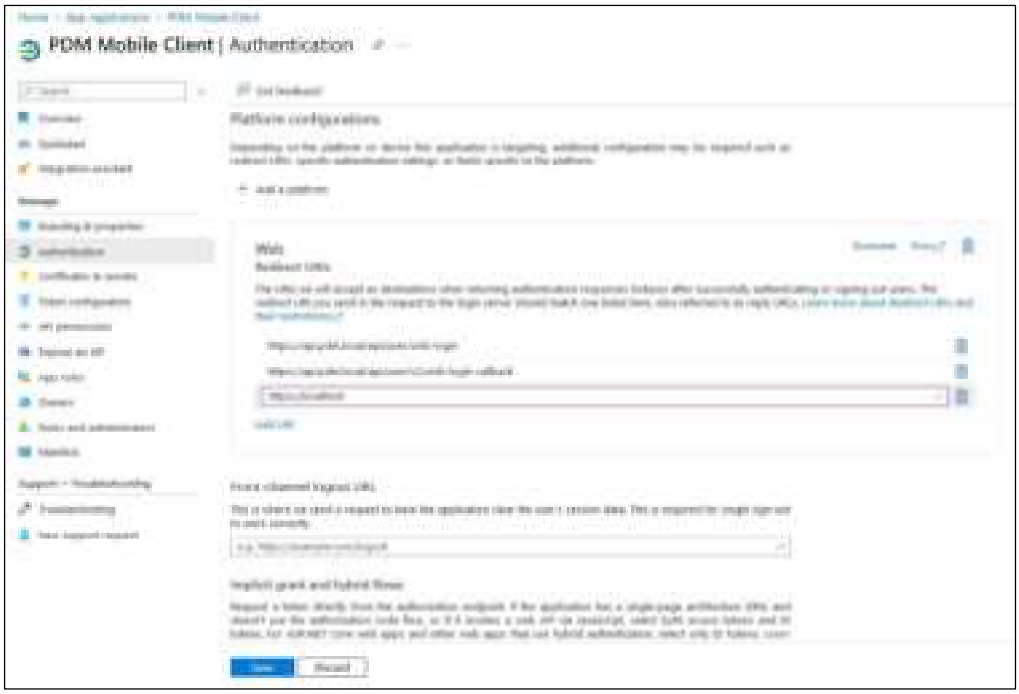
- Select ***ID tokens*** check box
- Click **[Configure]**.

→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



→ Enter the following details -

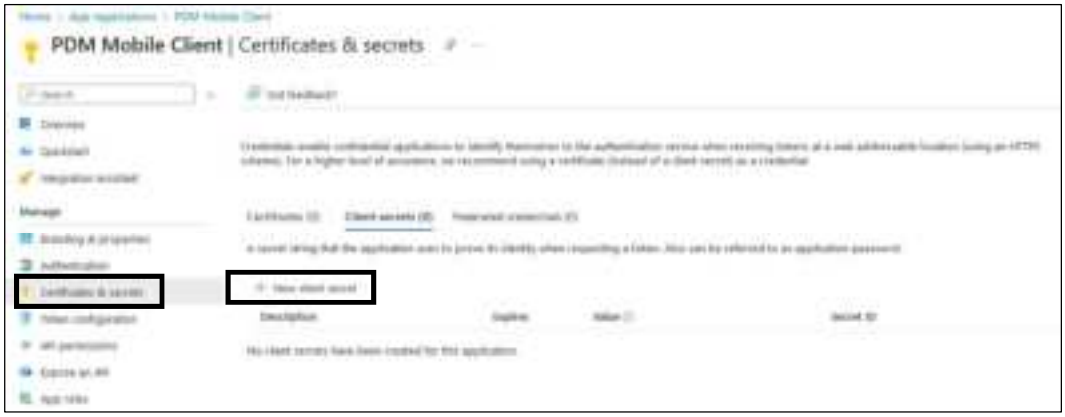
- **Redirect URIs** - PDM Login Redirect URI V2 – For example, *https://api.pdm.local/api/user/v2/oidc-login-callback*; *https://localhost* **(Mandatory).** The highlighted text indicates the domain name.
- *Front-channel logout URL*. (Optional).
- Select ***ID tokens*** check box



→ Upon adding the additional redirect URIs, click **[Save]**.

5.2.2.3.3 Setup Client Secret

→ In the left menu, select **Certificates & secrets**; click **+ New client secret**.



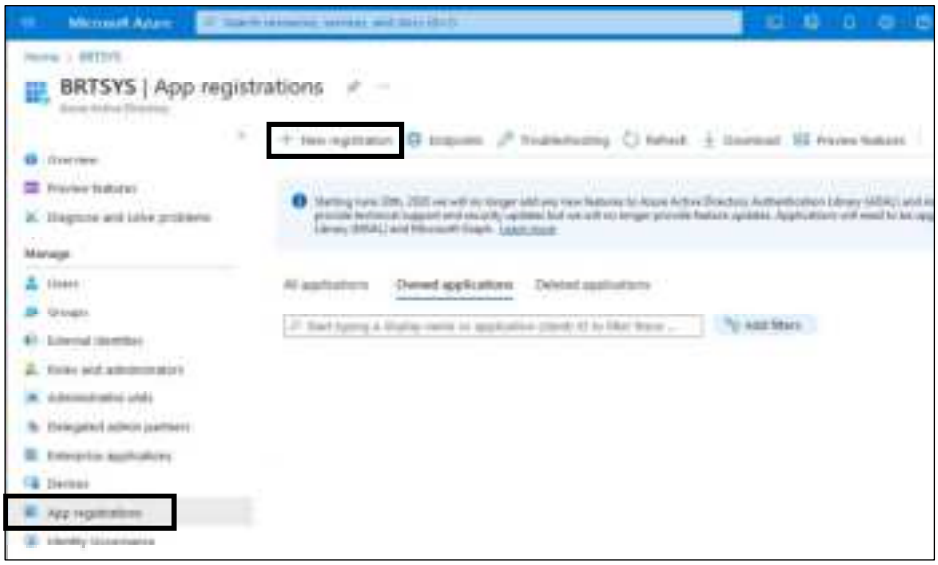
→ In the **Add a client secret UI**, enter the *Description*; choose an *expiration period* and click **[Add]**.

→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.

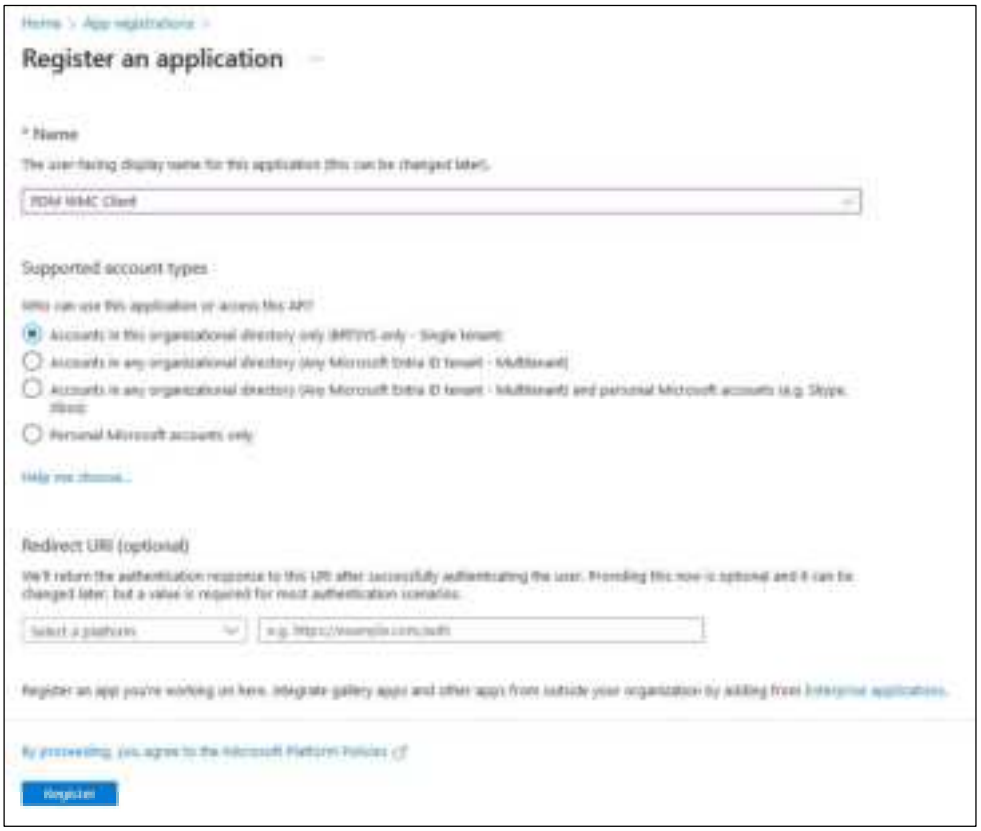
5.2.2.4 PDM Management Console (WMC Client)

5.2.2.4.1 App Registration

→ Select **App registrations**. Click **+ New registration**.



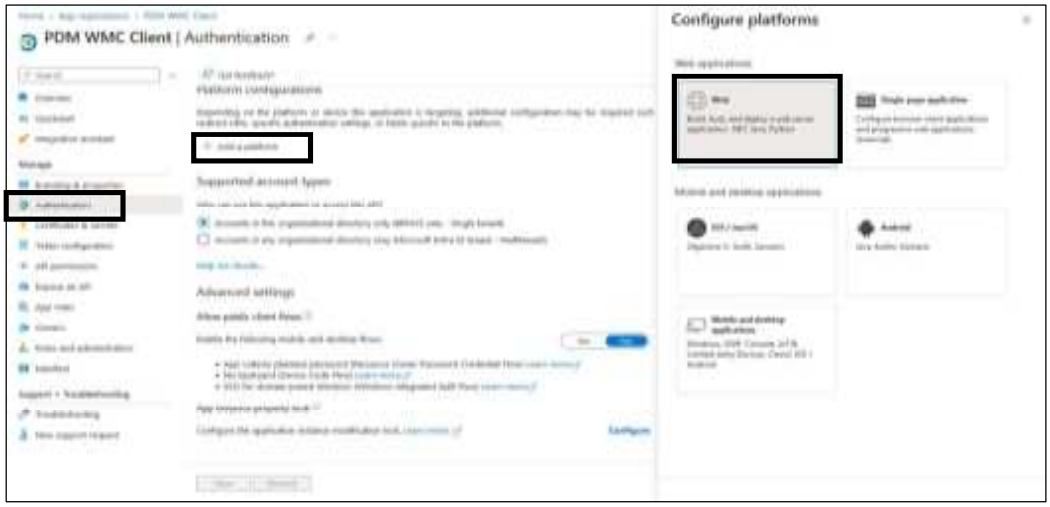
→ Enter the ***Application name*** **–** *PDM WMC Client*; select the ***Supported account types*** **–** *Accounts in this organisation directly only* from the available options. and click **[Register]**.



→ The PDM WMC Client application is successfully created.

5.2.2.4.2 Setup Authentication (Redirect URI)

→ Go to ***Authentication page*** and click on ***+ Add a platform***. Select **Web**.



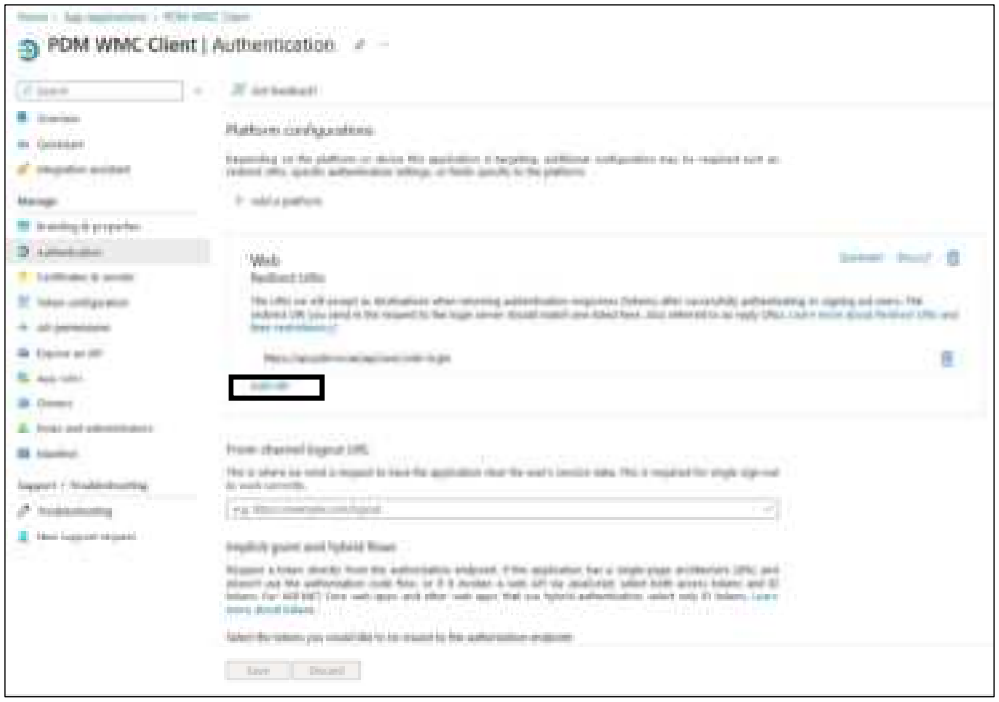
→ In the configure Web UI –

- Enter the **Redirect URIs** - PDM Login Redirect URI – For example, *https://api.pdm.local/api/user/oidc-login* **(Mandatory).**
- Enter the **Front-channel logout URL** - *https://api.pdm.local/api/user/single-logout*. This field is needed only when implementing single sign on. (Optional).

  pdm.local - indicates the domain name.

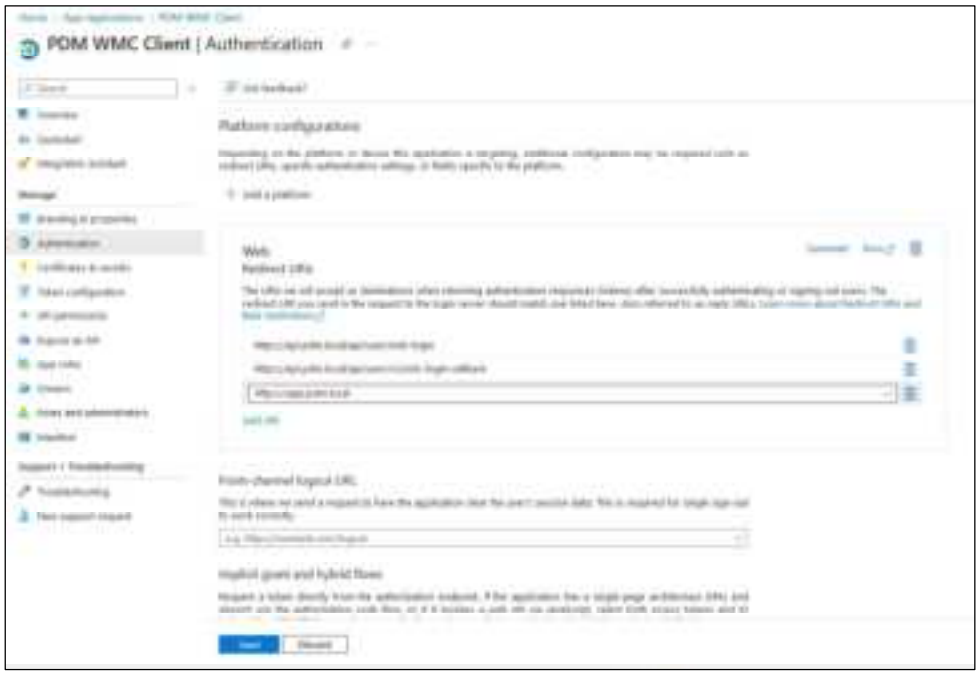
- Select ***ID tokens*** check box
- Click **[Configure]**.

→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



→ Enter the following details as part of the additional URLs -

- **Redirect URIs** - PDM Login Redirect URI V2 – For example, *https://api.pdm.local/api/user/v2/oidc-login-callback*; *https://app.pdm.local* **(Mandatory).** The highlighted text indicates the domain name.
- *Front-channel logout URL*. (Optional).
- Select ***ID tokens*** check box

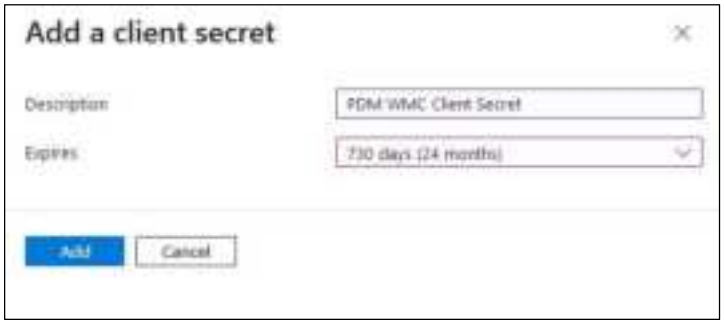


→ Upon adding the additional redirect URIs, click **[Save]**.

5.2.2.4.3 Setup Client Secret

→ In the left menu, select **Certificates & secrets**; click **+ New client secret**.

→ In the **Add a client secret UI**, enter the *Description*; choose an *expiration period* and click **[Add]**.

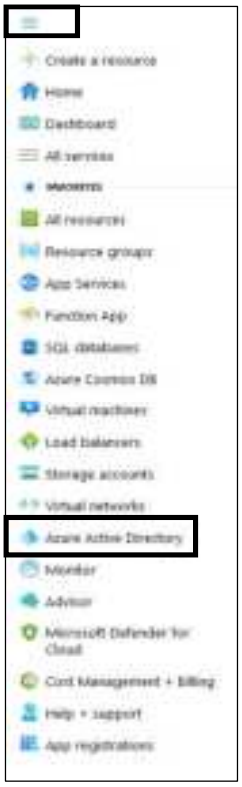


→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.

5.2.3 Modern Authentication using OAuth 2.0 - ROPC

→ Access Azure Portal using the administrator account – https://portal.azure.com.

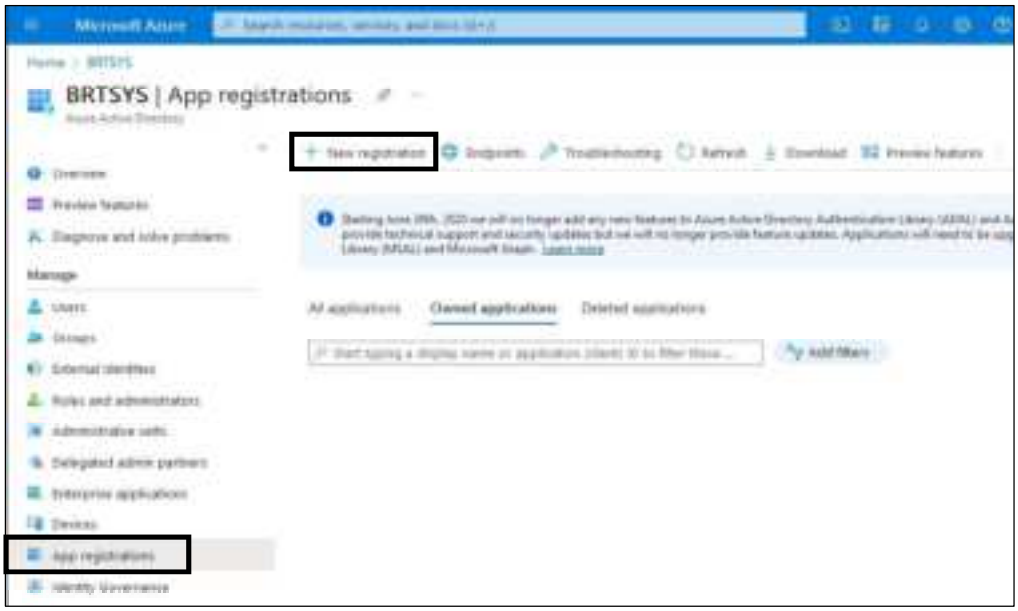
→ Go to **Azure Active Directory** from the left navigation menu.



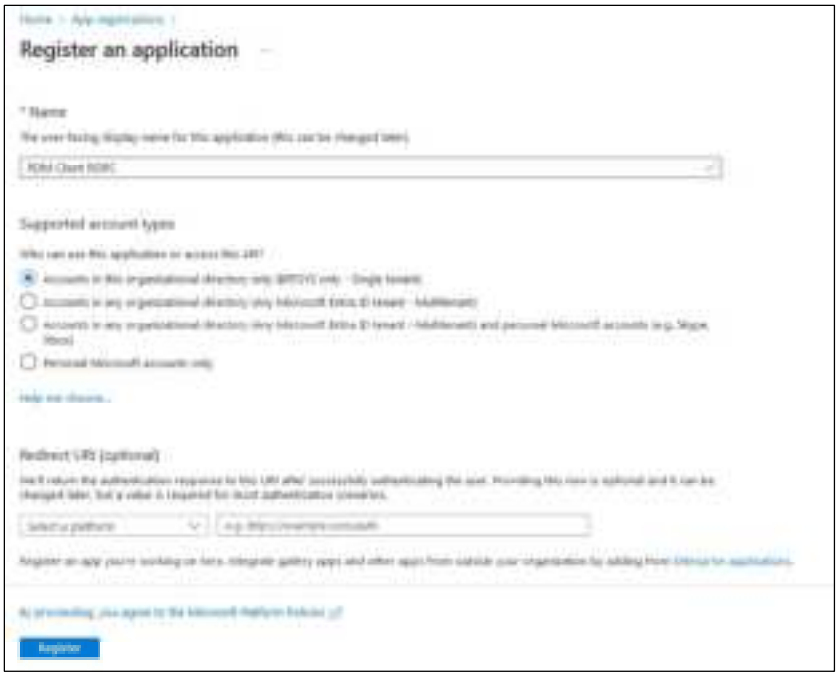
5.2.3.1 PDM Client

5.2.3.1.1 App Registration

→ Select **App registrations**. Click **+ New registration**.



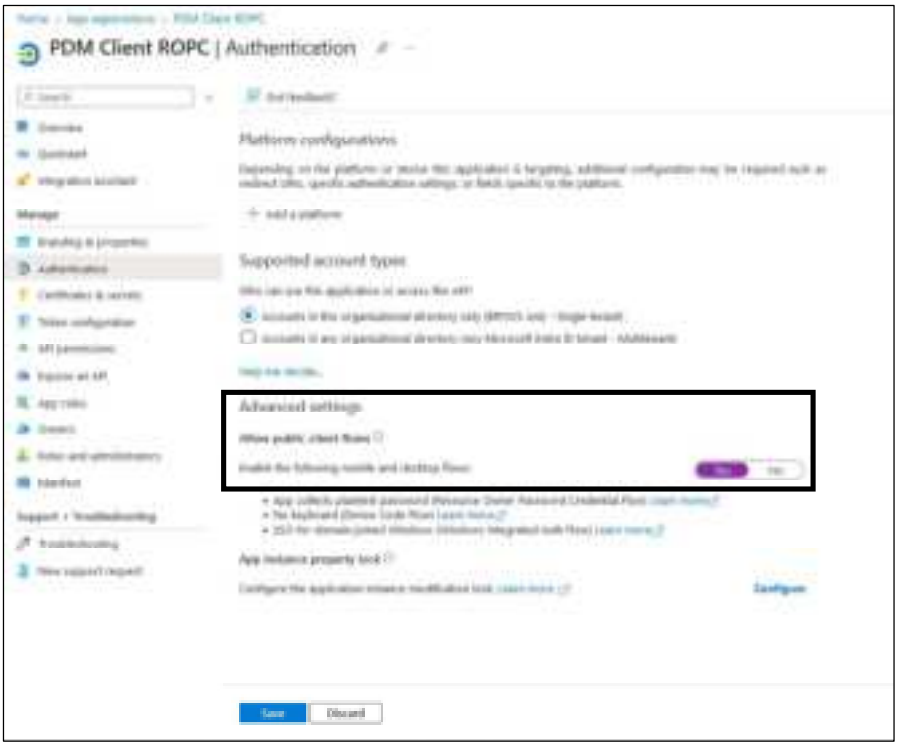
→ Enter the ***Application name –*** *PDM Client ROPC*; select the ***Supported account types –*** *Accounts in this organization directly only* from the available options. and click **[Register]**.



→ The PDM Client ROPC application is successfully created.

5.2.3.1.2 Setup Authentication

→ Go to ***Authentication page*** and set ***Advanced setting > Allow public client flows*** to *Yes*.

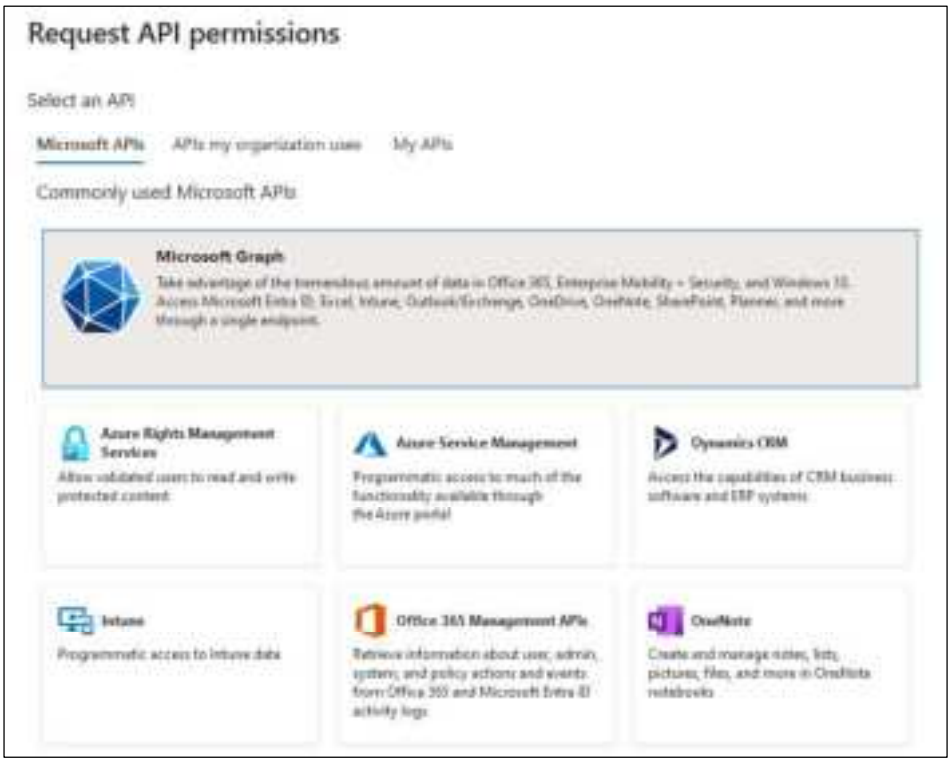


→ Click **[Save]**.

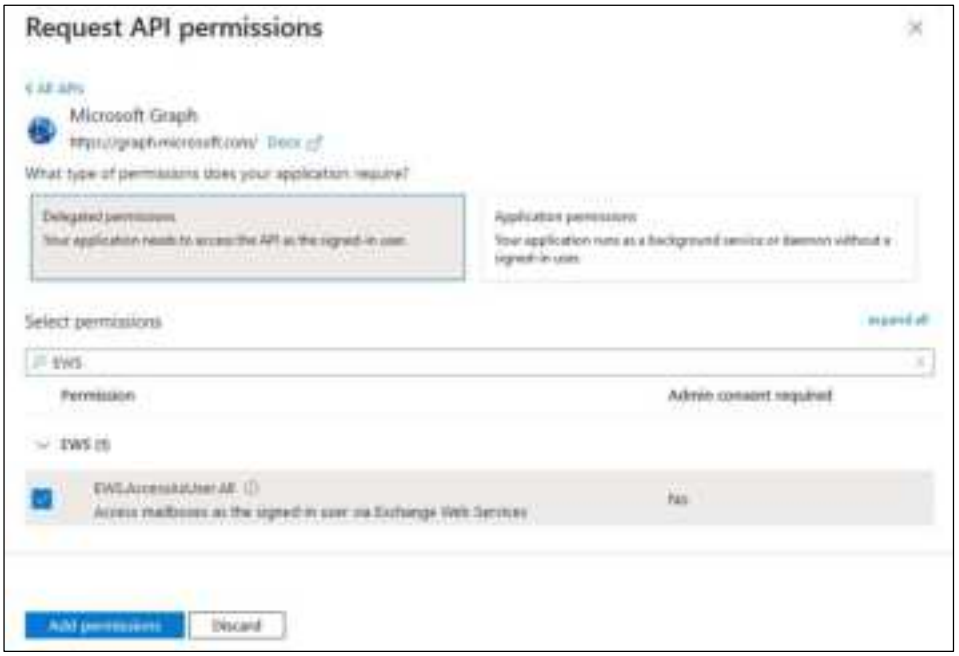
5.2.3.1.3 Setup API Permissions

→ From left navigation menu, go to ***API permissions*** → + ***Add a permission***.

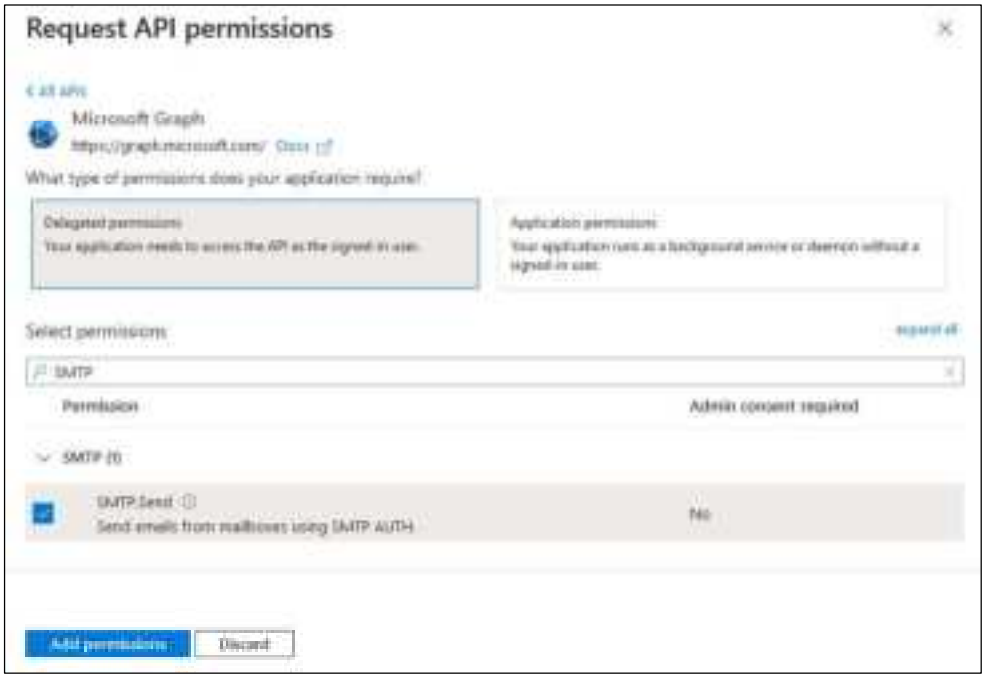
→ From the Request API permissions UI, click ***Microsoft APIs*** and select ***Microsoft Graph***.



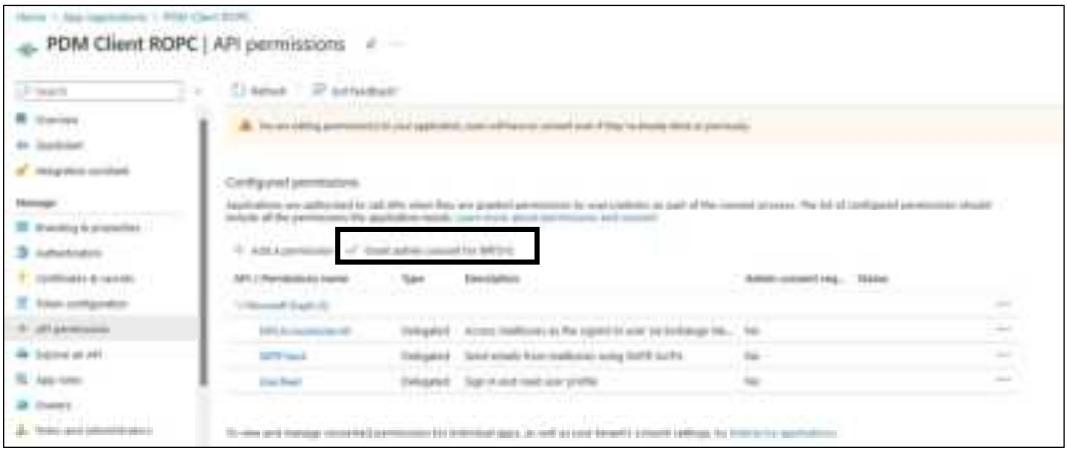
→ Select ***Delegated permissions***; ***Select permissions – EWS*** *(EWS.AccessAsUser.All)*. Click **[Add permissions]**.



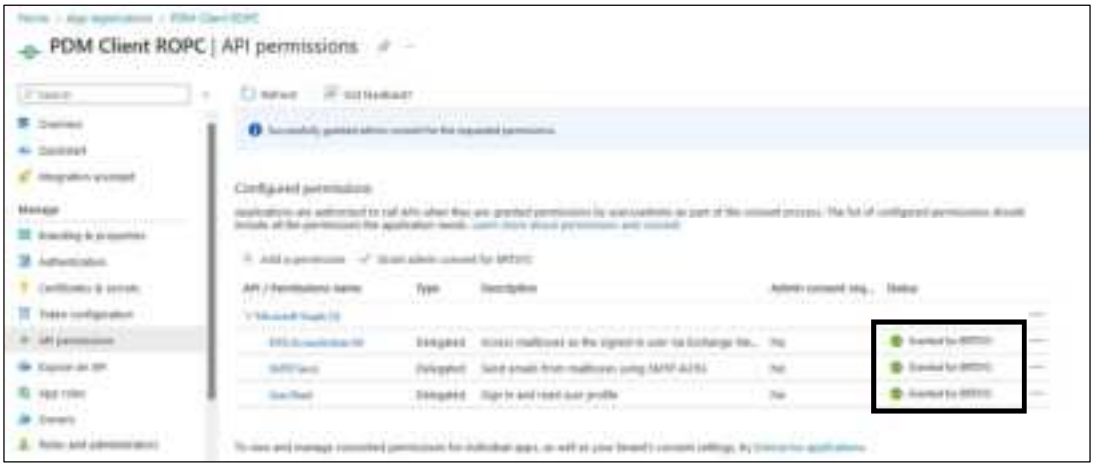
→ Select ***Delegated permissions***; ***Select permissions – SMTP*** (*SMTP.Send*). Click **[Add permissions]**.



→ The Office365 administrator must grant the permissions to be added. Click ***Grant admin consent for BRTSYS***. Click **[Yes]** to confirm.



→ Upon successfully granting permission, a green check mark will appear.



6. Appendix

6.1 Exchange Server setup using Exchange Management Shell – Quick Reference

→ **Open Exchange Management PowerShell as an Administrator**	a. From the exchange server, click **Start** → **Microsoft Exchange Server** → **Exchange Management Shell.** Right-click Exchange Management Shell and select **"Run as administrator"**. b. The *Exchange Management Shell* is opened. 
→ **Create User Account**	c. Create user account using the following command **–** `New-Mailbox -Name "User1" -DisplayName "User1" -UserPrincipalName "user1@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)`
→ **Create Distribution Group for Users**	PDM requires users to be identified by distribution groups (for example, *user1@bridgetek.com*). When creating User Groups, omit the *RoomList* parameter as it is not required. d. Create a new user distribution group named *"pdm-user-group-<groupname>"* using the following command - `New-DistributionGroup -Name "pdm-user-group-bridgetek1"`
	Note: A distribution group name should begin with prefix *pdm-user-group* and be followed by the group name.

	e. Add a user account *(user1@bridgetek.com)* to an existing user distribution group list *(pdm-user-group-bridgetek1)* using the following command **–**
	
	`Add-DistributionGroupMember -Identity "pdm-user-group-bridgetek1" -Member user1@bridgetek.com`
	
	f. Use the following command to display a list of users who have been added to a particular distribution group **–**
	
	`Get-DistributionGroupMember -Identity "pdm-user-group-bridgetek1"`

→ **Create Desk / Resource Account**	g. Using the following command, create a resource account **–** `New-Mailbox -Name "Desk1" -DisplayName "Desk1" -Room`
→ **Create Distribution Group for Desks**	PDM requires desks to be identified by distribution groups (for example, *desk1@bridgetek.com*). When creating User Groups, omit the *RoomList* parameter as it is not required.

	h. Create a new desk distribution group named *"pdm-desk-group-<groupname>"* using the following command - `New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList`
	Note: A distribution group name should begin with prefix *pdm-desk-group* and be followed by the group name.

	i. Add a resource account *(desk1@bridgetek.com)* to an existing desk list *(pdm-desk-group-bridgetek1)* using the following command –
	
	`Add-DistributionGroupMember -Identity "pdm-desk-group-bridgetek1" -Member desk1@bridgetek.com`
	
	j. Use the following command to display a list of desks that have been added to a particular distribution group –
	
	`Get-DistributionGroupMember -Identity " pdm-desk-group-bridgetek1"`

→ **Create Impersonation User / Service Account**	k. Create Service Account using the following command – `New-Mailbox -Name "service-account" -DisplayName "service-account" -UserPrincipalName "service-account@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)`

→ **Grant Service Account Impersonation Rights**	l. Create Admin Role Group and Grant Service Account Impersonation Rights using the following command –
	
	`New-RoleGroup -Name "Application Impersonation Role" -Roles "ApplicationImpersonation" -Members service-account@bridgetek.com`
	
	m. Using the following command, view the application impersonation data –
	
	`Get-ManagementRoleAssignment -Role "ApplicationImpersonation" -GetEffectiveUsers`

→ **Discovery Management**	n. Using the following command, add the service account into Discovery Management Role -
	
	`Add-RoleGroupMember -Identity "Discovery Management" -Member service-account@bridgetek.com`
	
	o. View the list of members in the Discovery Management Role, using the following command –
	
	`Get-RoleGroupMember -Identity "Discovery Management"`

6.2 Microsoft 365 setup using Windows PowerShell – Quick Reference

→ **Open Windows PowerShell as an Administrator**	a. Enter PowerShell in Search box, then right-click on the Windows PowerShell icon and Select **"Run as administrator"**.
	
	b. In the console, use the following command to install Exchange Online Management Module.
	
	`$Install-Module-Name ExchangeOnlineManagement`
	
	c. Using the following command, import the Exchange Online Management Module –
	
	`$ Import-Module ExchangeOnlineManagement`
	
	d. Using the following command connect to the Exchange Online Management Module.
	
	`Connect-ExchangeOnline -UserPrincipalName Administrator@bridgetek.com`
	
	Now the Microsoft 365 can be managed via PowerShell.

→ **Create User Account**	e. Create user account using the following command – `New-Mailbox -Name "User1" -DisplayName "User1" -UserPrincipalName "user1@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)`
→ **Create Distribution Group for Users**	PDM requires users to be identified by distribution groups (for example, *user1@bridgetek.com*). When creating User Groups, omit the *RoomList* parameter as it is not required. e. Create a new user distribution group named *"pdm-user-group-<groupname>"* using the following command - `New-DistributionGroup -Name "pdm-user-group-bridgetek1"`
	Note: A distribution group name should begin with prefix *pdm-user-group* and be followed by the group name.

	f. Add a user account *(user1@bridgetek.com)* to an existing user distribution group list *(pdm-user-group-bridgetek1)* using the following command –
	
	`Add-DistributionGroupMember -Identity "pdm-user-group-bridgetek1" -Member user1@bridgetek.com`
	
	g. Use the following command to display a list of users who have been added to a particular distribution group –
	
	`Get-DistributionGroupMember -Identity "pdm-user-group-bridgetek1"`

→ **Create Desk / Resource Account**	h. Using the following command, create a resource account – `New-Mailbox -Name "Desk1" -DisplayName "Desk1" -Room`

→ **Create Distribution Group for Desks**	PDM requires desks to be identified by distribution groups (for example, *desk1@bridgetek.com*). When creating User Groups, omit the *RoomList* parameter as it is not required. i. Create a new desk distribution group named *"pdm-desk-group-<groupname>"* using the following command - `New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList`
	Note: A distribution group name should begin with prefix *pdm-desk-group* and be followed by the group name.

	j. Add a resource account *(desk1@bridgetek.com)* to an existing desk list *(pdm-desk-group-bridgetek1)* using the following command –
	
	`Add-DistributionGroupMember -Identity "pdm-desk-group-bridgetek1" -Member desk1@bridgetek.com`
	
	k. Use the following command to display a list of desks that have been added to a particular distribution group –
	
	`Get-DistributionGroupMember -Identity " pdm-desk-group-bridgetek1"`

→ **Create Impersonation User / Service Account**	l. Create Service Account using the following command – `New-Mailbox -Name "service-account" -DisplayName "service-account" -UserPrincipalName "service-account@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)`

→ **Grant Service Account Impersonation Rights**	m. Create Admin Role Group and Grant Service Account Impersonation Rights using the following command –
	
	`New-RoleGroup -Name "Application Impersonation Role" -Roles "ApplicationImpersonation" -Members service-account@bridgetek.com`
	
	n. Using the following command, view the application impersonation data –
	
	`Get-ManagementRoleAssignment -Role "ApplicationImpersonation" -GetEffectiveUsers`

→ **Discovery Management**	o. Using the following command, add the service account into Discovery Management Role -
	
	`Add-RoleGroupMember -Identity "Discovery Management" -Member service-account@bridgetek.com`
	
	p. View the list of members in the Discovery Management Role, using the following command –
	
	`Get-RoleGroupMember -Identity "Discovery Management"`

6.3 Glossary of Terms, Acronyms & Abbreviations

Term or Acronym	Definition or Meaning
API	An Application Programming Interface, is a set of defined rules that enable different applications to communicate with each other.
DNS	The Domain Name System is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks.
EWS	An Embedded Web Server is an HTTP server used in an embedded system.
IP	The Internet Protocol is the network layer communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
MMC	Microsoft Management Console is a component of Microsoft Windows that provides system administrators and advanced users an interface for configuring and monitoring the system
PDM	PanL Desk Manager is a desk booking system that addresses the desk resource allocation problems by enabling organizations to automatically manage hotdesks.
RAM	Random Access Memory is a form of electronic computer memory that can be read and changed in any order, typically used to store working data and machine code.
RHEL	Red Hat Enterprise Linux is an enterprise Linux operating system (OS) developed by Red Hat for the business market
ROPC	The Resource Owner Password Credentials grant is designed for obtaining access tokens directly in exchange for a username and password.
SSL	Secure Sockets Layer is an encryption-based Internet security protocol.
SMTP	The Simple Mail Transfer Protocol is an Internet standard communication protocol for electronic mail transmission
URI	A Uniform Resource Identifier is a unique sequence of characters that identifies a logical or physical resource used by web technologies.
URL	A Uniform Resource Locator, colloquially known as an address on the Web, is a reference to a resource that specifies its location on a computer network and a mechanism for retrieving it.

6.4 List of Figures

NA

6.5 List of Tables

Revision History

Document Title	:	BRTSYS_AN_045 PDM User Guide - 2. Installation and Configuration
Document Reference No.	:	BRTSYS_000116
Clearance No.	:	BRTSYS#077
Product Page	:	https://brtsys.com/pdm/
Document Feedback	:	Send Feedback

Revision	Changes	Date
Version 1.0	Initial release for PanL Desk Manager (PDM) V2.6.0	28-07-2023
Version 2.0	Updated release for PanL Desk Manager (PDM) V3.1.0	01-07-2024