

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	4
2. Intended Audience	4
3. Document References	4
4. PDM Server Installation & Configuration	5
4.1 Hardware / Software Requirements	5
4.2 Network Port Requirements.....	5
4.3 Installing PDM on Linux-Distribution Server.....	6
4.3.1 System Requirements	6
4.3.2 Pre-Installation Procedure	6
4.3.3 Installing PDM Server Software.....	7
4.3.4 Update PDM Server Software Package.....	8
4.3.5 Change the current SSL Certificate and Domain Name	9
4.3.6 Un-install PDM Server Software Package	10
4.4 Domain Name Configuration	11
4.5 SSL Certificate Setup	13
5. Mail/Calendar Server Setup & Configuration	14
5.1 Exchange Server 2019/2016 / 2013 Setup	14
5.1.1 Using Exchange Admin Centre Console	15
5.2 Microsoft 365 Setup.....	26
5.2.1 Using Microsoft 365 Admin Center Console	27
5.2.2 Modern Authentication using OAuth 2.0 – Open ID-Connect (OIDC)	38
5.2.2.1 PDM Client	38
5.2.2.1.1 App Registration	38
5.2.2.1.2 Setup Authentication (Redirect URI).....	40
5.2.2.1.3 Setup Client Secret	41
5.2.2.1.4 Setup API Permissions.....	42
5.2.2.1.5 Setup Delegate Permissions.....	44
5.2.2.2 Add-In Client.....	47
5.2.2.2.1 App Registration	47
5.2.2.2.2 Setup Authentication (Redirect URI).....	48
5.2.2.2.3 Setup Client Secret	50
5.2.2.3 Mobile Client	51
5.2.2.3.1 App Registration	51
5.2.2.3.2 Setup Authentication (Redirect URI).....	52
5.2.2.3.3 Setup Client Secret	54
5.2.2.4 PDM Management Console (WMC Client).....	55
5.2.2.4.1 App Registration	55
5.2.2.4.2 Setup Authentication (Redirect URI).....	56
5.2.2.4.3 Setup Client Secret	58
5.2.3 Modern Authentication using OAuth 2.0 - ROPC	59
5.2.3.1 PDM Client	59
5.2.3.1.1 App Registration	59
5.2.3.1.2 Setup Authentication	61
5.2.3.1.3 Setup API Permissions.....	61
6. Appendix	65
6.1 Exchange Server setup using Exchange Management Shell – Quick Reference	65
6.2 Microsoft 365 setup using Windows PowerShell – Quick Reference.....	67
6.3 Glossary of Terms, Acronyms & Abbreviations	69

6.4	List of Figures	69
6.5	List of Tables	69
Revision History		70

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		
	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
Network Ports	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.



- [illegible]

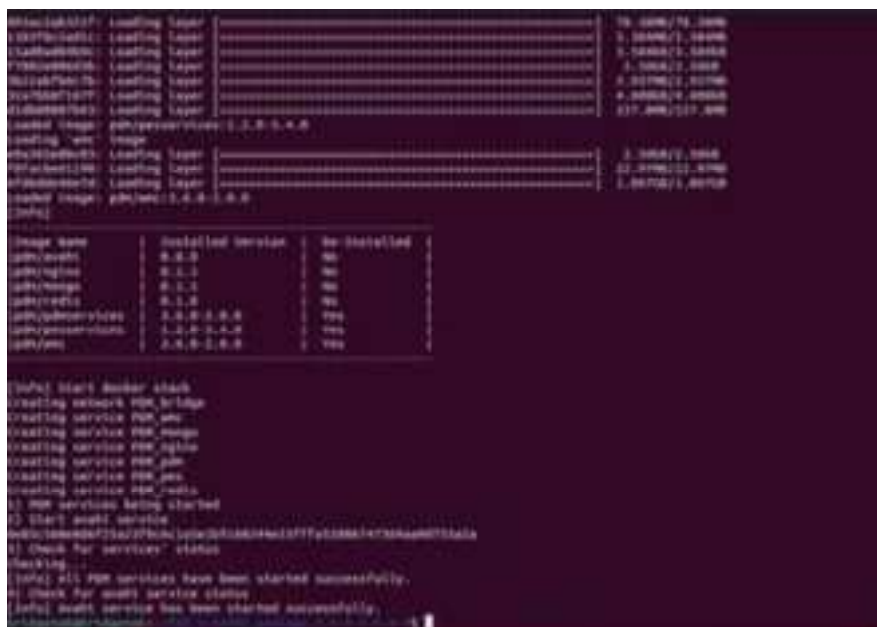
[illegible]

- [illegible]

[illegible]

- Copyright © BRT Systems Pte Ltd

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



Package Name	Installed Version	Is Installed
pdm	2.0.0	Yes
pdm/bridge	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes
pdm/psm	2.0.0	Yes

- 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
```


4.4 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>

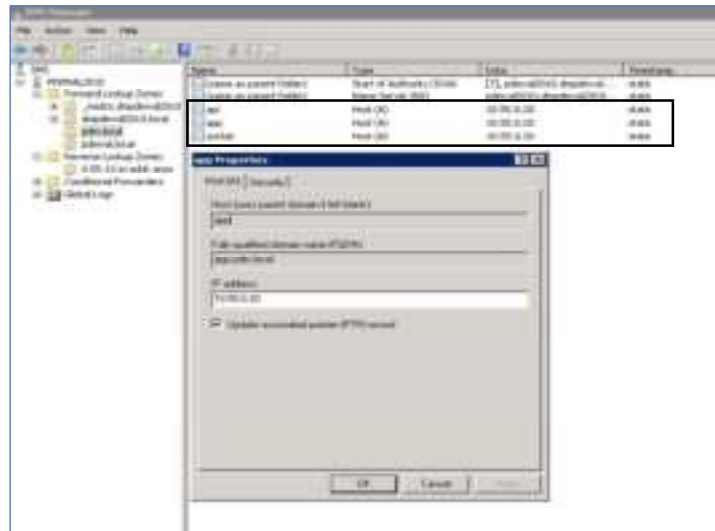
where in the *domain name* refers to the *organization's domain name*. For example, if the organization's name is ABC Pte Ltd, then the domain name can be abc.com or abc.local.

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

- Local DNS Server
- Global DNS Service

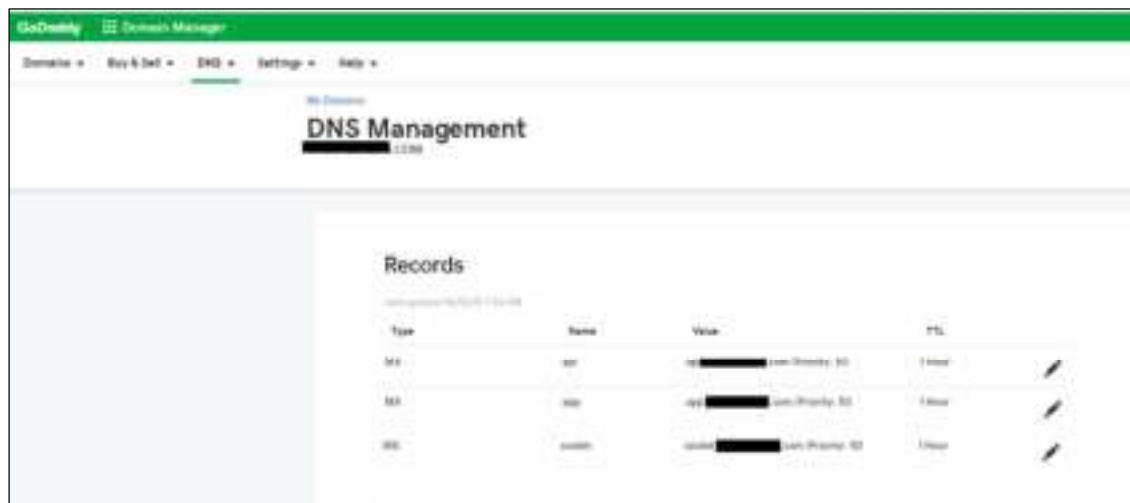
Local DNS

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-



The screenshot shows the GoDaddy DNS Management interface. The top navigation bar includes links for Domain, Buy & Sell, DNS, Settings, and Help. The main heading is "DNS Management". Below this, there is a "Records" section with a table of DNS records. The table has columns for Type, Name, Value, TTL, and an edit icon. Three records are listed: A, MX, and NS.

Type	Name	Value	TTL	
A	api	api [redacted] com (Priority: 0)	1 hour	
MX	api	api [redacted] com (Priority: 0)	1 hour	
NS	api	ns1 [redacted] com (Priority: 0)	1 hour	

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 -> <i>Configuration</i> -> <i>System</i>".

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



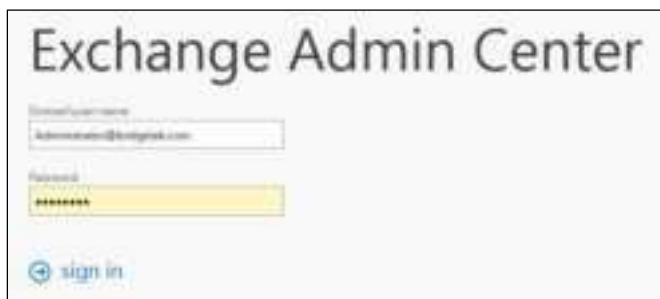
Note: Refer to the steps given under [Appendix > Exchange Server setup using Exchange Management Shell – Quick Reference](#) for more details.

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.

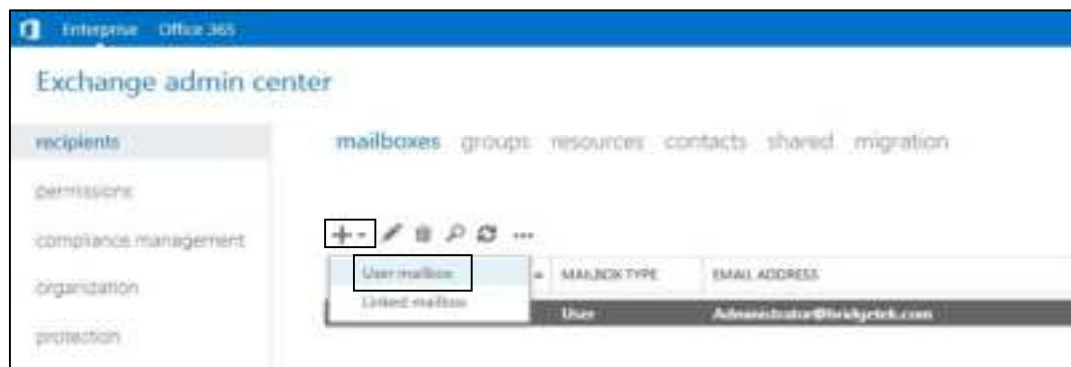


→ Create User Account

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



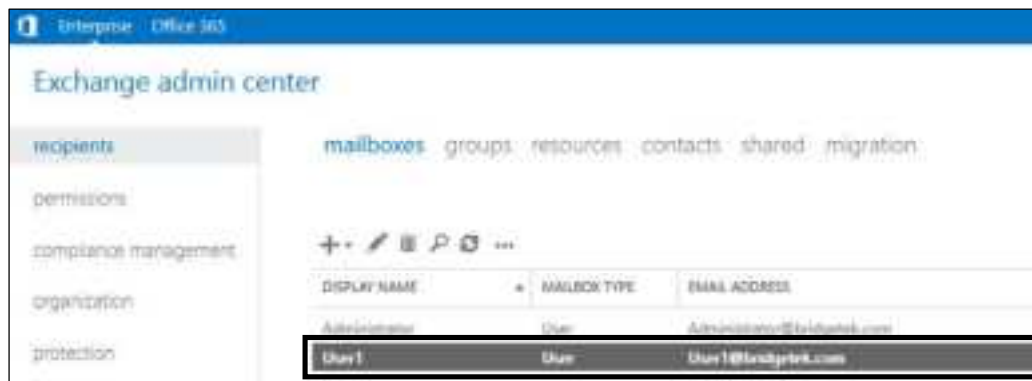
- Click **"+"** and select **"User mailbox"**.



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



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



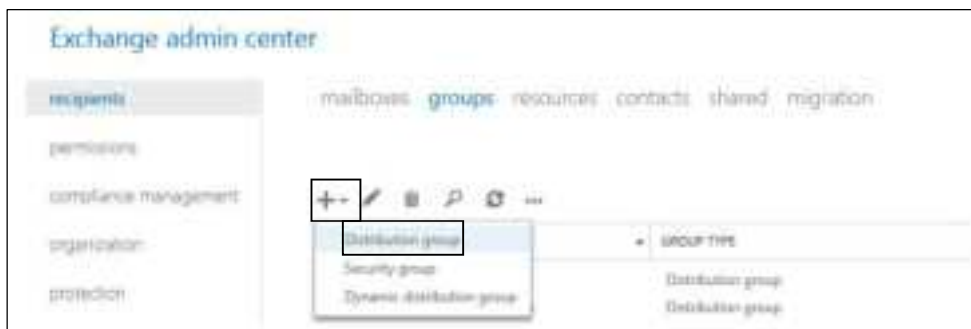
DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@brtsys.com
User1	User	User1@brtsys.com

→ Create Distribution Group for Users

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



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



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

new distribution group

*Display name
pdm-user-group-1@bgelek1

*Alias
pdm-user-group-1@bgelek1

Notes

Organizational unit
Browse...

*Owners
+ -
Administrator

Members
☒ Add group owners as members
+ -

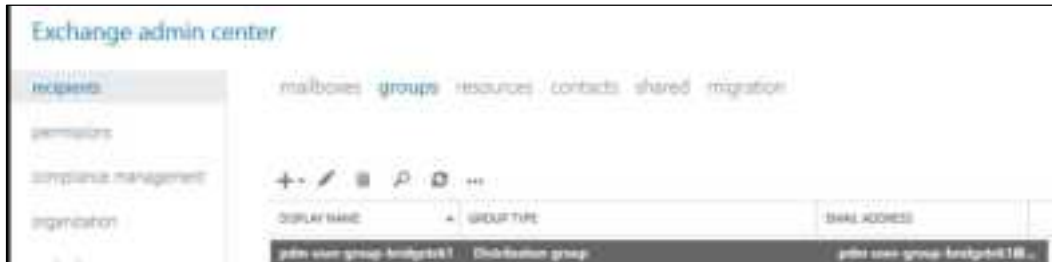
Click Add to add members to this group. Members will receive a copy of messages sent to the group.

Choose whether owner approval is required to join the group.
☒ Open: Anyone can join this group without being approved by the group owners.
☐ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.
☐ Owner approval: All requests are approved or rejected by the group owners.

Please do not publish this document to the Internet

Save Cancel

- The newly added distribution group is displayed.

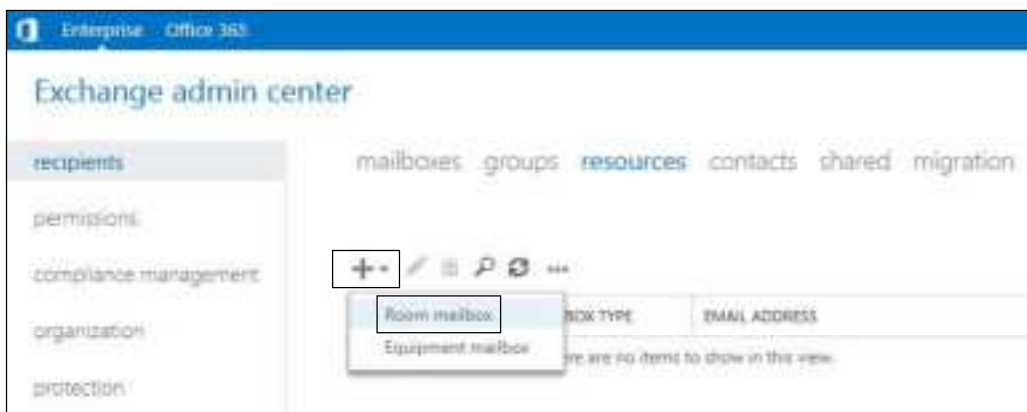


→ Create Desk / Resource Account

- 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.



DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Desk1	Room	Desk1@bridgetek.com

→ 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 -

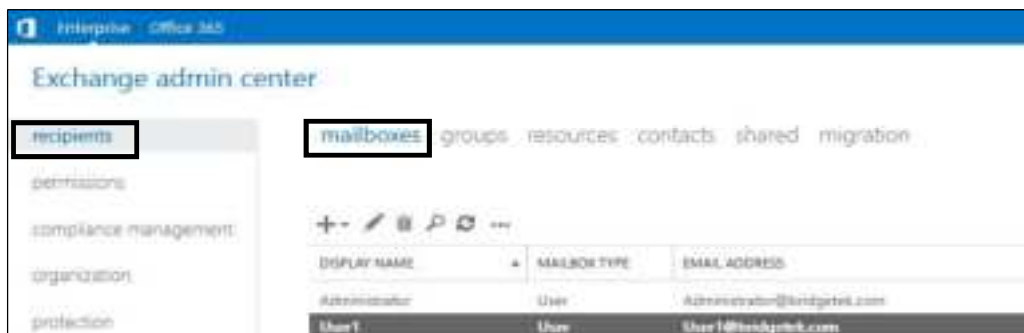
```
New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList
```



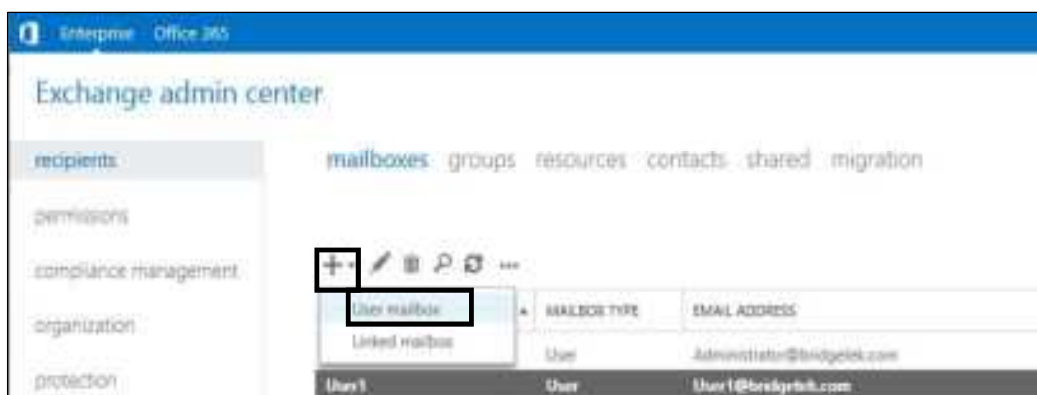
Note: A distribution group name should begin with prefix *pdm-desk-group* and be followed by the group name.

→ Create Impersonation User / Service Account

- Go to “recipients” → “mailboxes”.



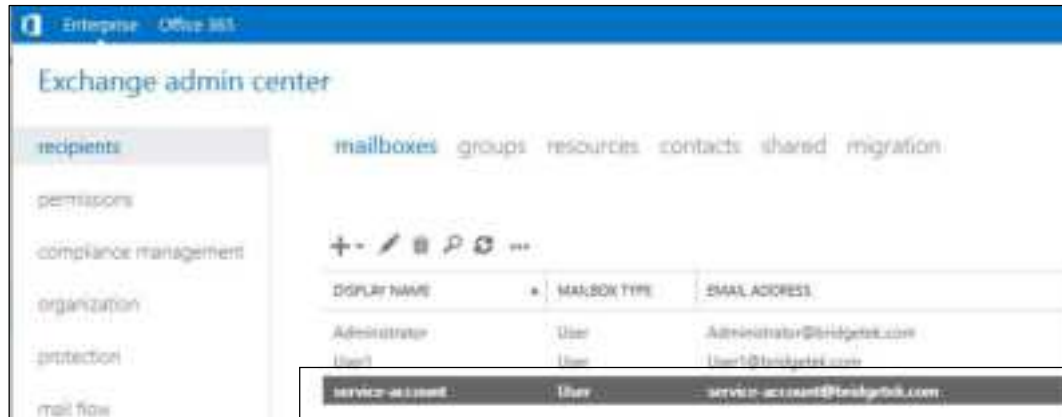
- Click + and select **User mailbox**.



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



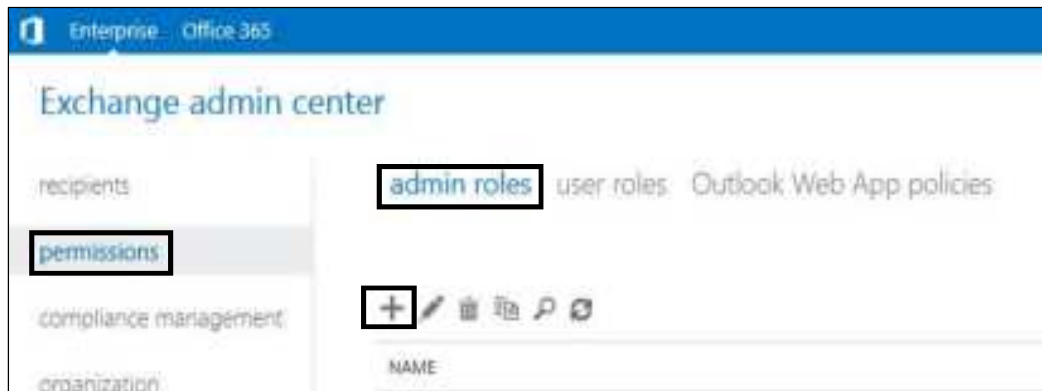
- The Service account will appear in the list of mailboxes.



→ 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).

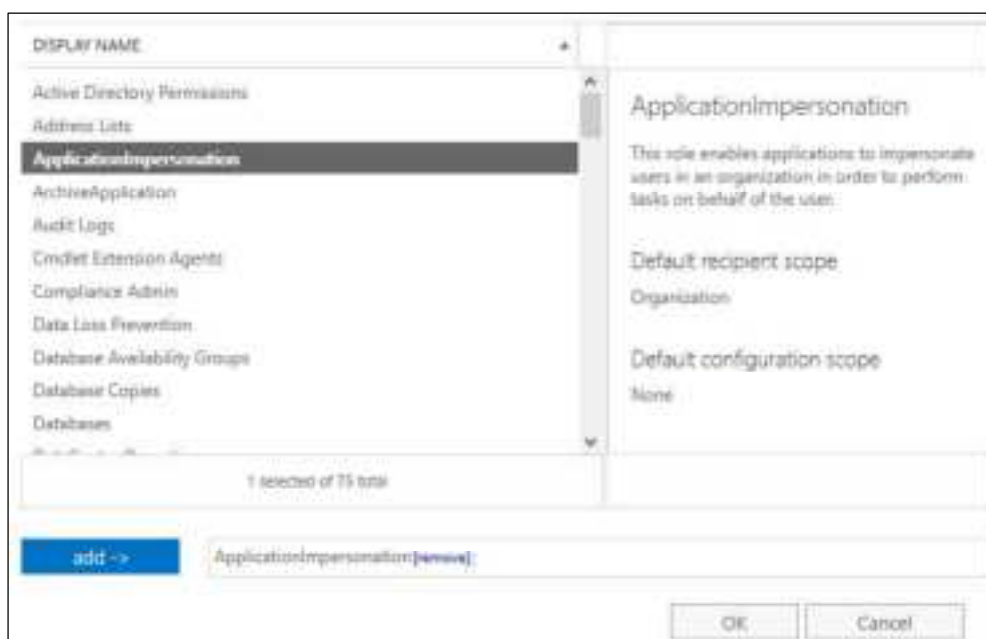


The screenshot shows the 'new role group' form. The 'Name' field is set to 'Application Impersonation Role'. The 'Description' field is empty. The 'Write scope' dropdown is set to 'Default'.

- 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].



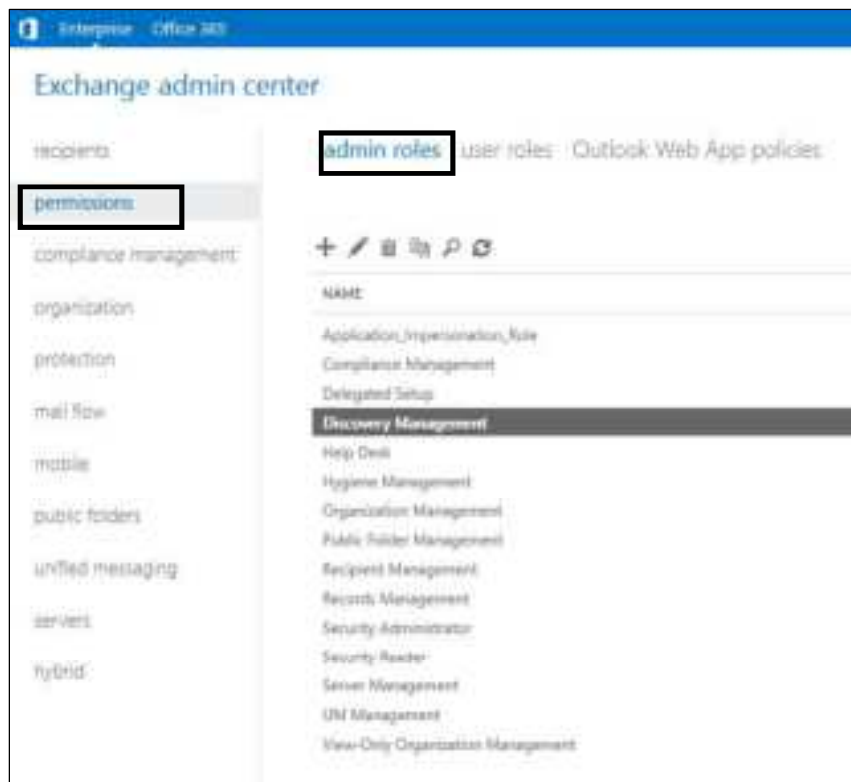
- The newly added role is displayed under the **"admin roles"**.



→ 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**.

Discovery Management

Name:
Discovery Management

Description:
Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:
☒ Default

Organizational unit:

Roles:
+ -

NAME
Exchange Mailbox Search
Mailbox Search
MailboxSearchApplication

Members:
+ -

NAME	DISPLAY NAME
pm-admin	pm-admin
pm-admin7	pm-admin7
pm-admin8	pm-admin8
pm-admin9	pm-admin9
service-account	Service Account

Save Cancel

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

Members:

+ -

NAME	DISPLAY NAME
service-account	Service Account

Save Cancel

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 -> <i>Configuration</i> -> <i>System</i>".

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 –

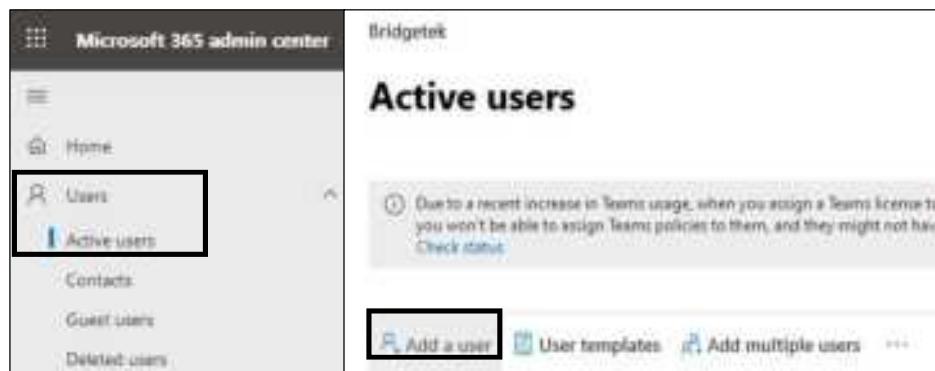
→ Login to Microsoft 365 Admin Center Console

- Go to the [Microsoft 365 Admin center](#) and log in with Microsoft 365 admin account.



→ Create User Account

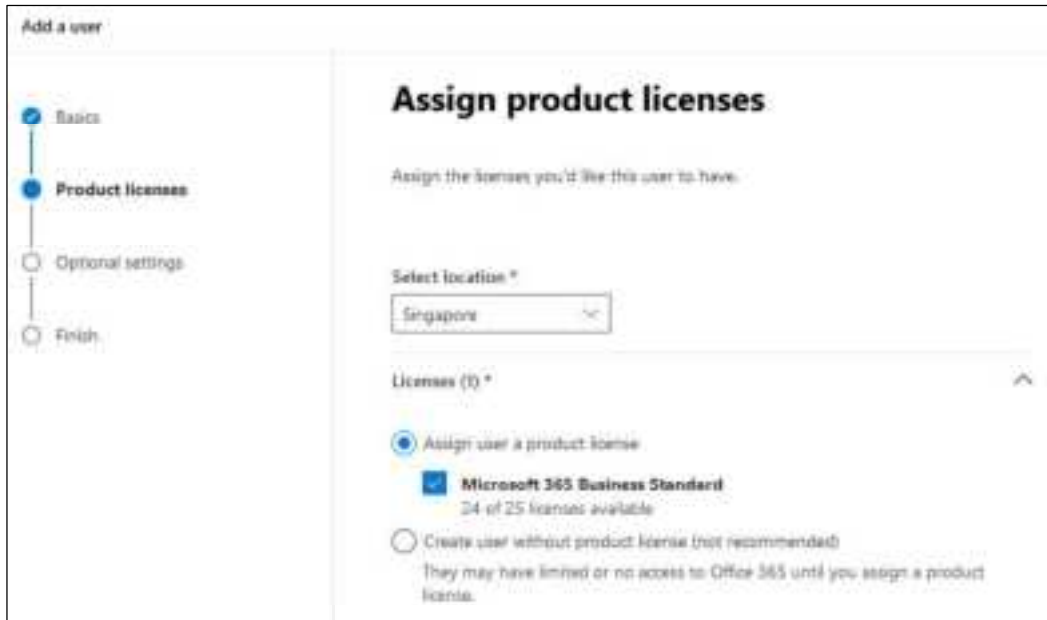
- In the Microsoft 365 admin centre, click **"Users → Active Users → Add a user"**.



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

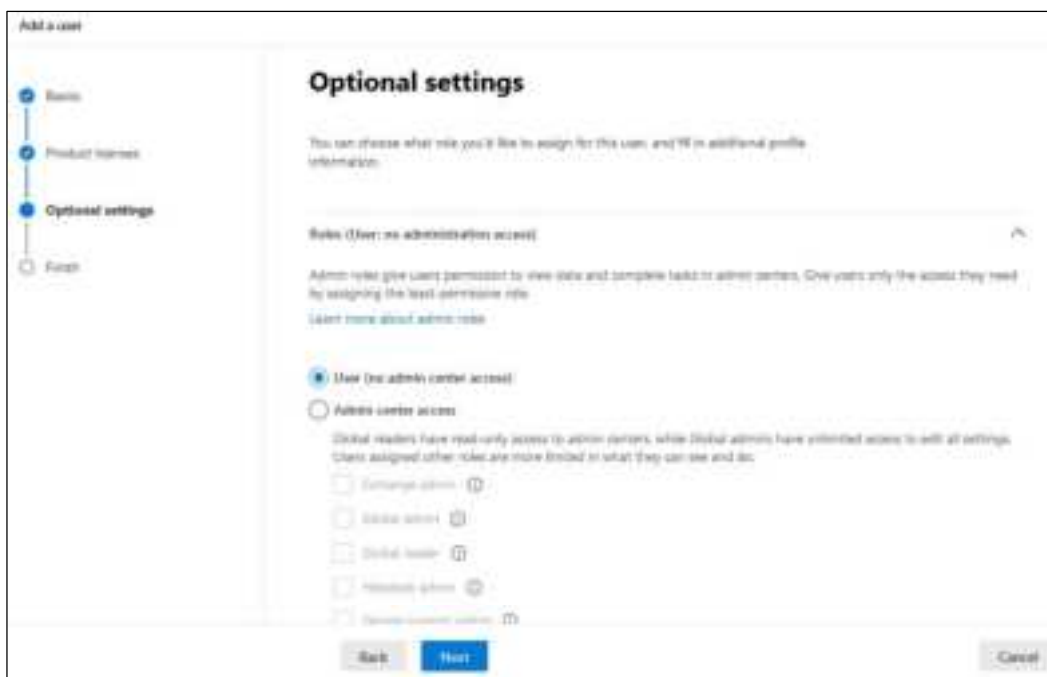


- Assign the “**product licenses**”. Click **[Next]**.



The screenshot shows the 'Assign product licenses' step in the 'Add a user' wizard. On the left, a progress bar indicates the steps: Basics, Product licenses (current), Optional settings, and Finish. The main content area has the title 'Assign product licenses' and the instruction 'Assign the licenses you'd like this user to have.' Below this, there is a 'Select location *' dropdown menu with 'Singapore' selected. Under the 'Licenses (0) *' section, there are two radio button options. The first option, 'Assign user a product license', is selected. It includes a blue checkmark icon and the text 'Microsoft 365 Business Standard' with '24 of 25 licenses available' below it. The second option is 'Create user without product license (not recommended)', which includes a warning that 'They may have limited or no access to Office 365 until you assign a product license.'

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



The screenshot shows the 'Optional settings' step in the 'Add a user' wizard. On the left, the progress bar shows: Basics, Product licenses, Optional settings (current), and Finish. The main content area has the title 'Optional settings' and the instruction 'You can choose what role you'd like to assign for this user, and fill in additional profile information.' Below this, there is a 'Roles (User: no administration access)' section. It explains that 'Admin roles give users permission to view data and complete tasks in other centers. Give users only the access they need by assigning the least permissive role. Learn more about admin roles.' There are two radio button options: 'User (no admin center access)' (selected) and 'Admin center access'. Under 'Admin center access', there is a list of roles with checkboxes: 'Exchange admin', 'Global admin', 'Global reader', 'Read-only global admin', and 'SharePoint admin'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

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

Add a user

- Basics
- Product licenses
- Optional settings
- Finish

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
User1
user1@bridgeek.com
[Edit](#)

Password
Type Custom password
Send To: Administrator@bridgeek.com
[Edit](#)

Product licenses
Licenses: Singapore
Licenses: Microsoft 365 Business Standard
Apps: Power Virtual Agents for Office 365, Common Data Service for Teams, Project for Office (Plan E3), 23 more
[Edit](#)

Roles (default)
User (no admin control access)

[Back](#)
[Finish adding](#)
[Cancel](#)

Add a user

- Basics
- Product licenses
- Optional settings
- Finish



User1 added to active users

User1 will now appear in your list of active users.

User details
Display name: User1
Username: user1@bridgeek.com
Password: ***** [Show](#)
Sending to: Administrator@bridgeek.com

Licenses brought
None

Licenses assigned
Microsoft 365 Business Standard

Save these user settings as a template?

User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.

[Review settings for this user template.](#)

[Close](#)

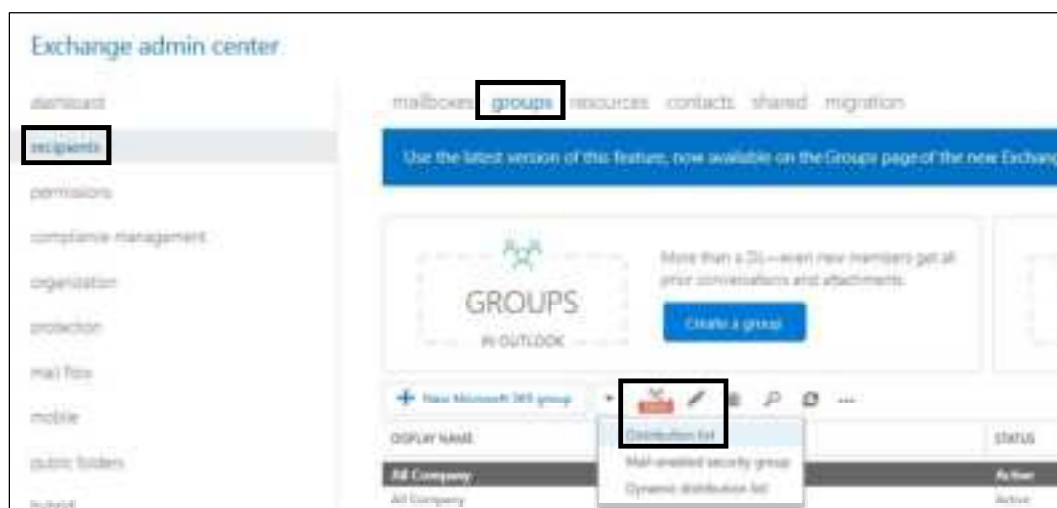
The user account details are added to active users list.



Display name	Username	License
Administrator Bridgetek	Administrator@bridgetek.com	Microsoft 365 Business Standard
Room1	Room1@bridgetek.com	Unlicensed
service_account	service_account@bridgetek.com	Microsoft 365 Business Standard
User1	user1@bridgetek.com	Microsoft 365 Business Standard

→ 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]**.



new distribution list

*Display name
john-sm-group-bdgedist1

*Alias
john-sm-group-bdgedist1

*Email address
john-sm-group-bdgedist1 @ mkttest1.onmicrosoft.com

Notes

*Owners
+ -

Administrator

Members
+ Add group members (members)

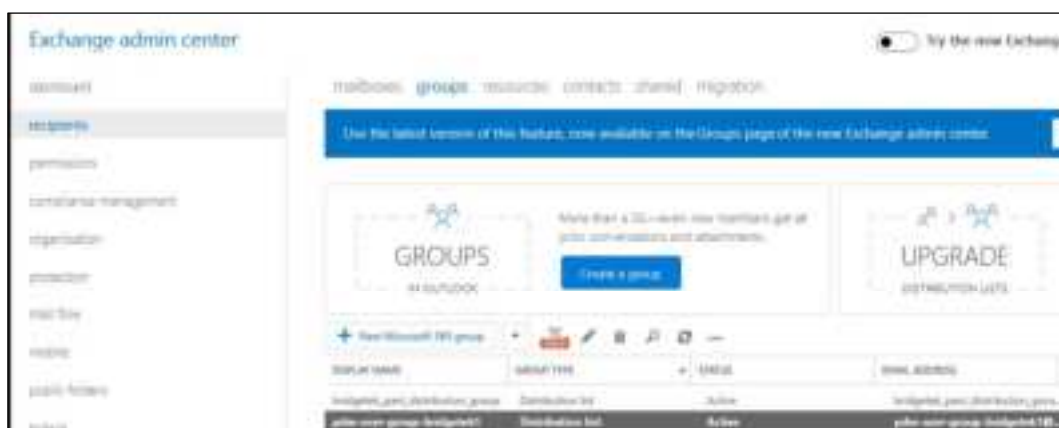
+ -

Click Add to add members to this group. Members will receive a copy of messages sent to the group.

Choose whether group approval is required to join the group.
☒ Open: Anyone can join this group without being approved by the group owners.
☐ Closed: Members can be added only by the group owners. All requests to join will be rejected automatically.
☐ Owner approval: All requests are approved or rejected by the group owners.

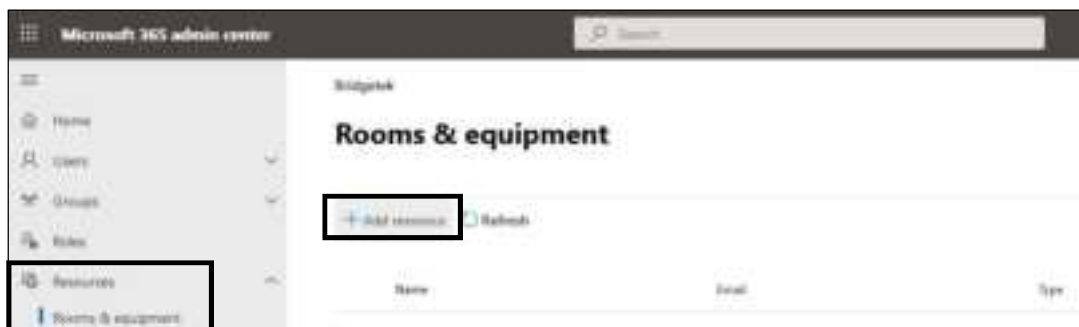
Save Cancel

- 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]**.

Add resource

Create a mailbox for things like a conference room, company car, or equipment that everyone needs to use, so that those resources are reservable.

[Learn more about resource types](#)

Resource type

Room

Name *

Desk1

The resource name appears in the address book and in the To and From lines in meeting invitations and responses.

Email *

Desk1

Domains

@ bridgetek.com

The email address is used to send meeting invitations to the resource.

Capacity

1

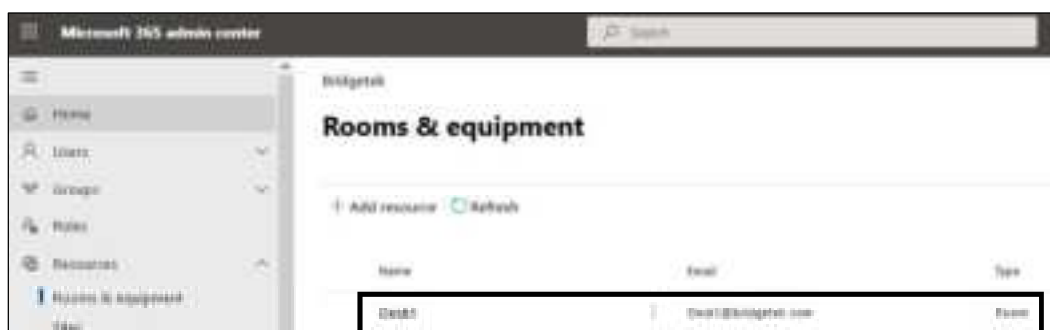
The number of people who can fit in the room or use the equipment at the same time.

Location

SG-07-03

Save

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

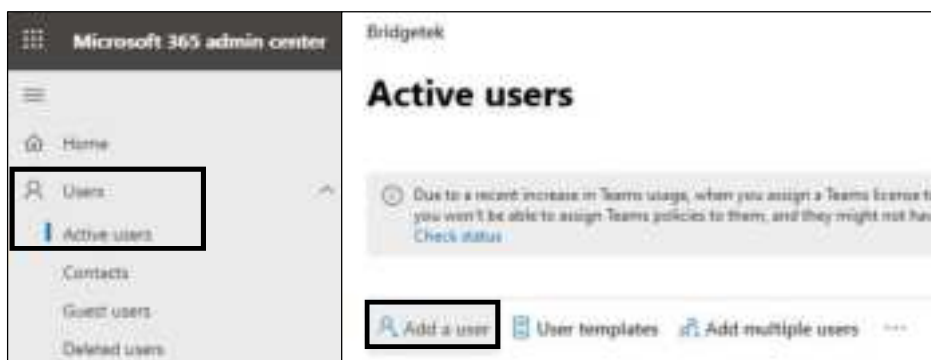


→ Create Distribution Group for Desks

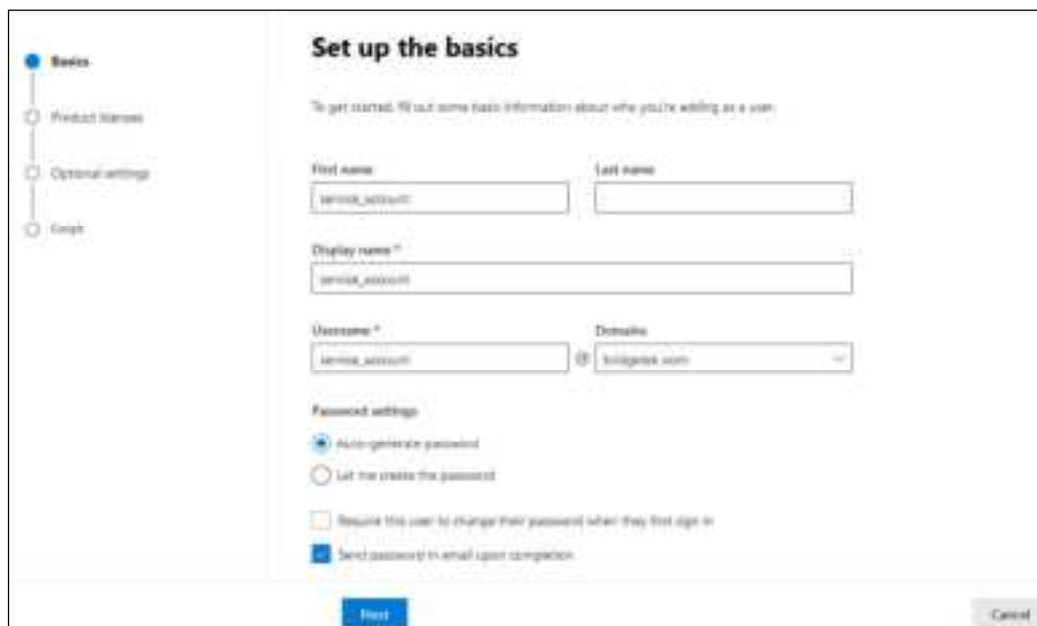
The distribution group for Rooms (RoomList) can be created **only** using the [Exchange PowerShell](#).

→ 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]**.



Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name: Last name:

Display name:

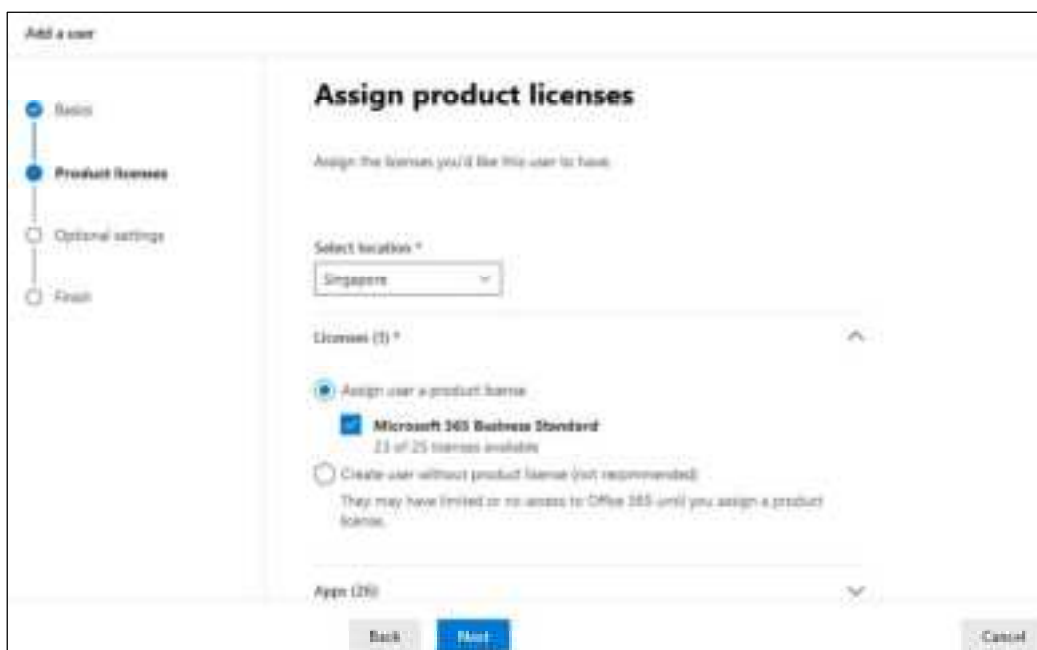
Username: Password:

Password settings:

- ☒ Auto-generate password
- ☐ Let the user create the password
- ☐ Require this user to change their password when they first sign in
- ☒ Send password to email upon completion

Next **Cancel**

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



Assign product licenses

Assign the licenses you'd like this user to have.

Select location:

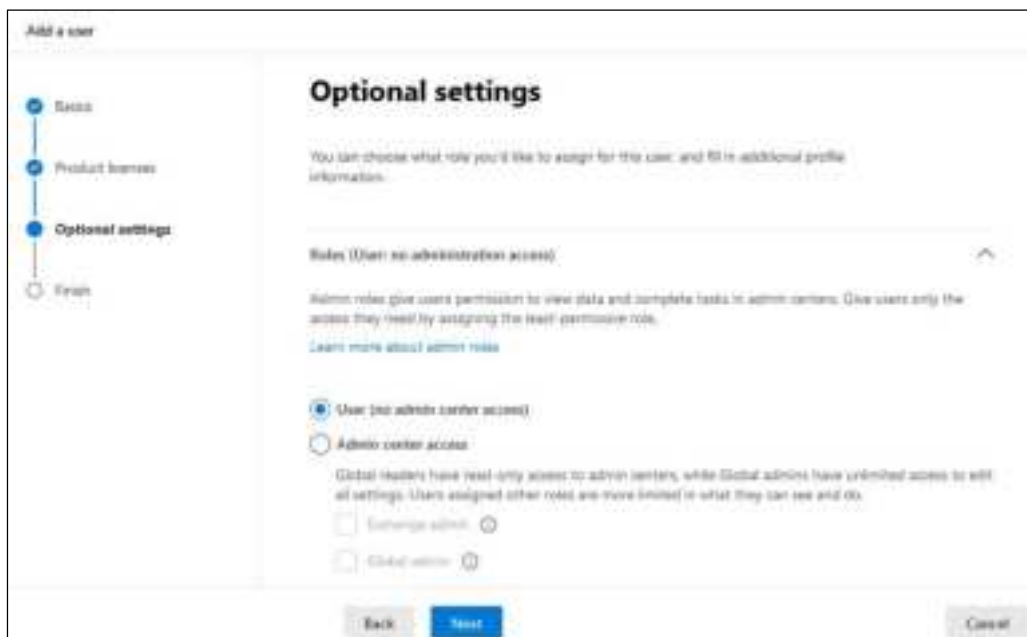
Licenses (1):

- ☒ Assign user a product license
 - ☒ **Microsoft 365 Business Standard**
23 of 25 licenses available
 - ☐ Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

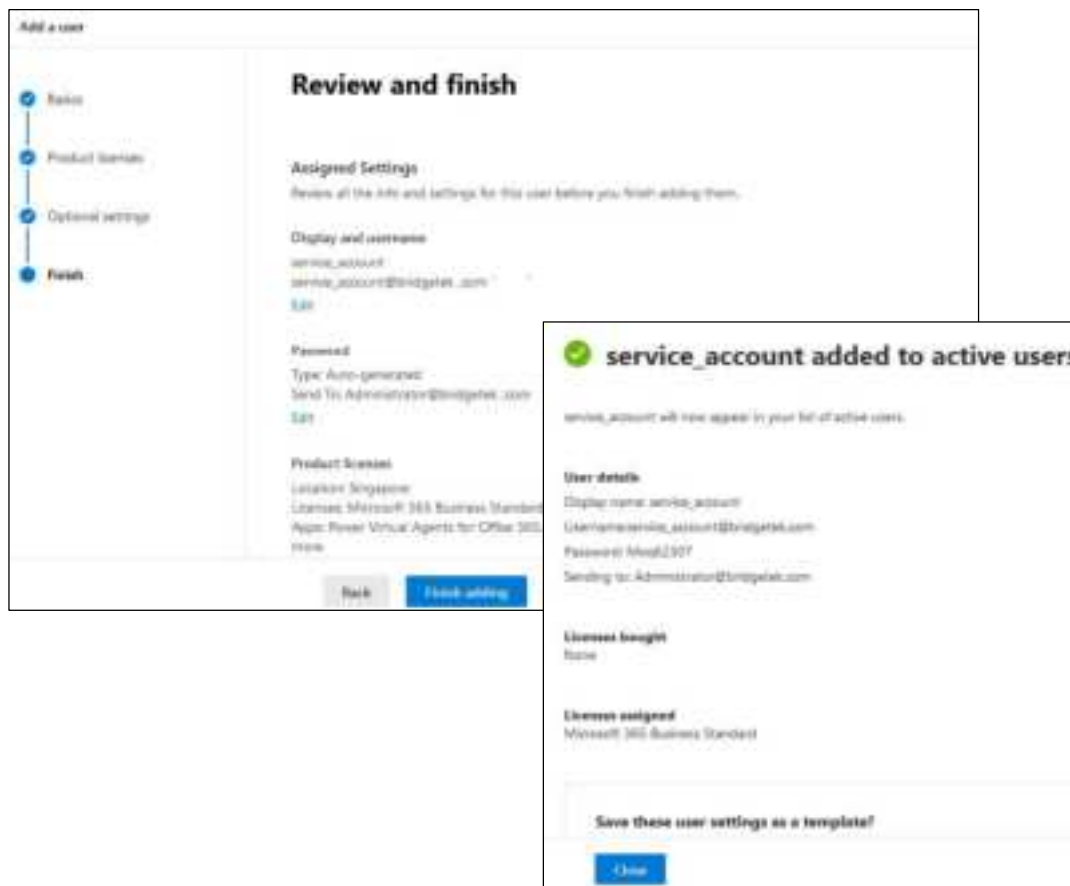
Apps (28)

Back **Next** **Cancel**

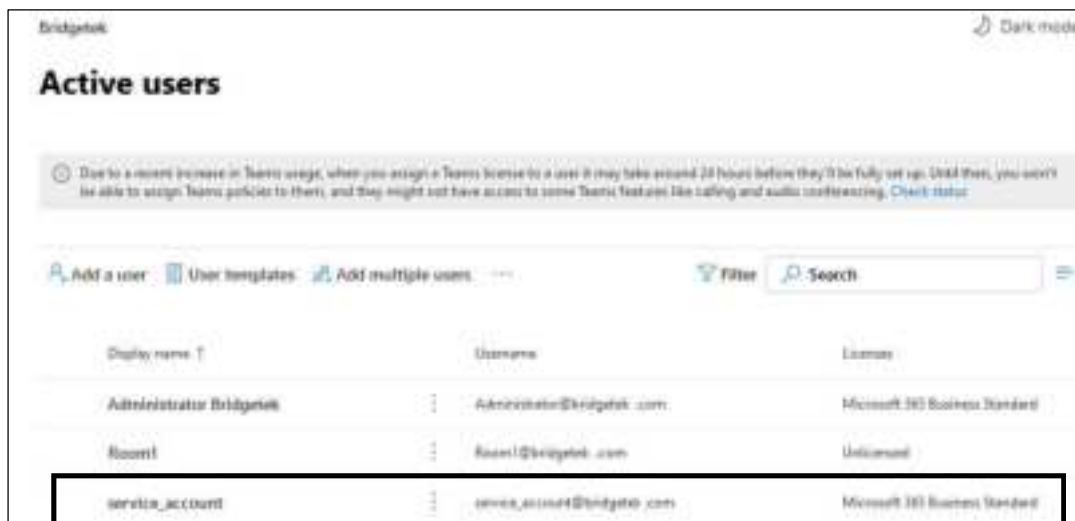
- Go through the **Optional settings** and select as required. Click **[Next]**.



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



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

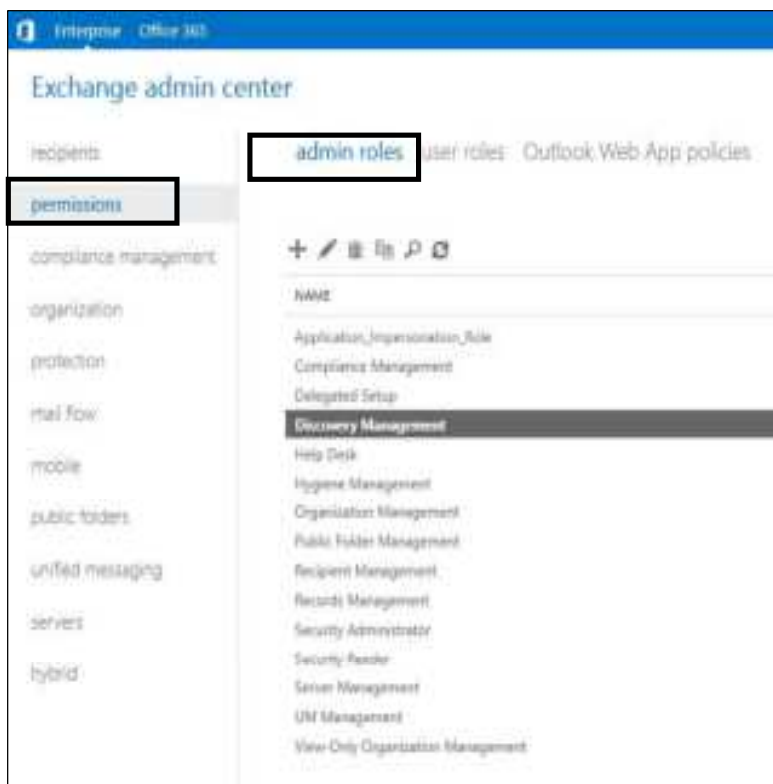


→ Granting Service Account Impersonation Rights

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**.



Discovery Management

Name:
Discovery Management

Description:
Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

Write scope:
☒ Default

Organizational unit:

Rules:
+ -

NAME
Legal Hold
Mailbox Search
MailboxSearchApplication

Members:
+ -

NAME	DISPLAY NAME
pm-admin	pm-admin
pm-admin7	pm-admin7
pm-admin8	pm-admin8
pm-admin9	pm-admin9
SERVICE ACCOUNT	SERVICE ACCOUNT

Save Cancel

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



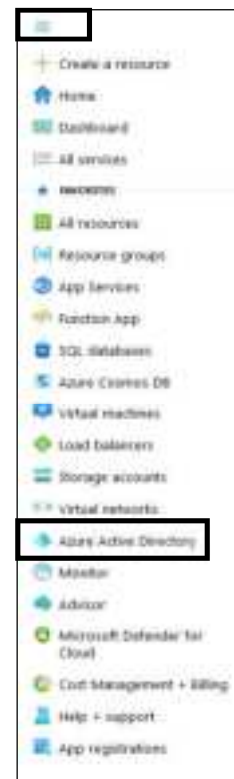
Members:
+ -

NAME	DISPLAY NAME
Service Account	Service Account

Save Cancel

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

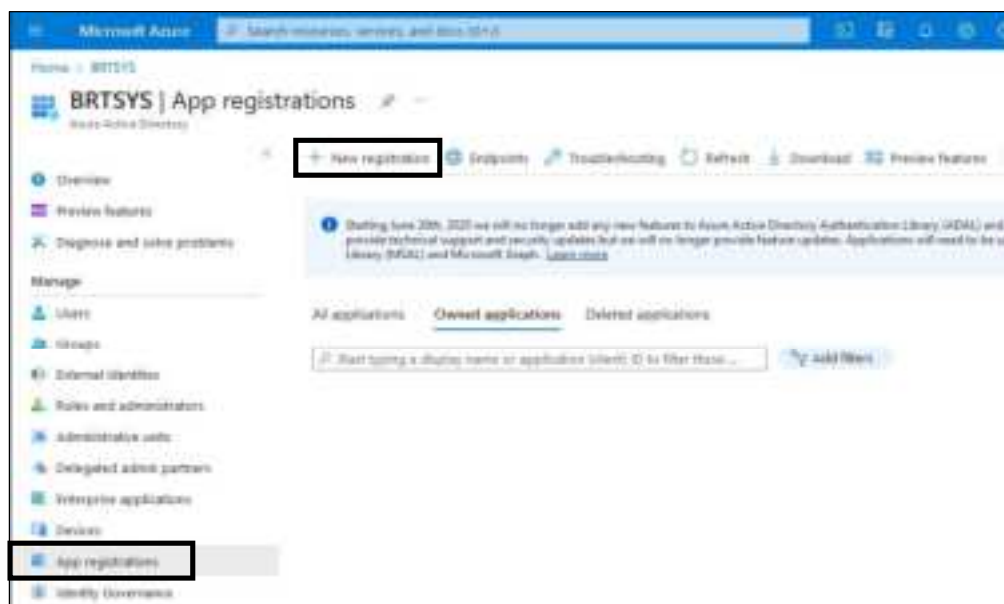
- Access Azure Portal using the administrator account - <https://portal.azure.com>
- Go to **Azure Active Directory** from the left navigation menu.
 - Register Applications
 - Setup Authentication (Redirect URI)
 - Setup Client Secret
 - Setup API Permissions



5.2.2.1 PDM Client

5.2.2.1.1 App Registration

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



- 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 the API?

☒ Accounts in the organizational directory only (B2B101 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...](#)

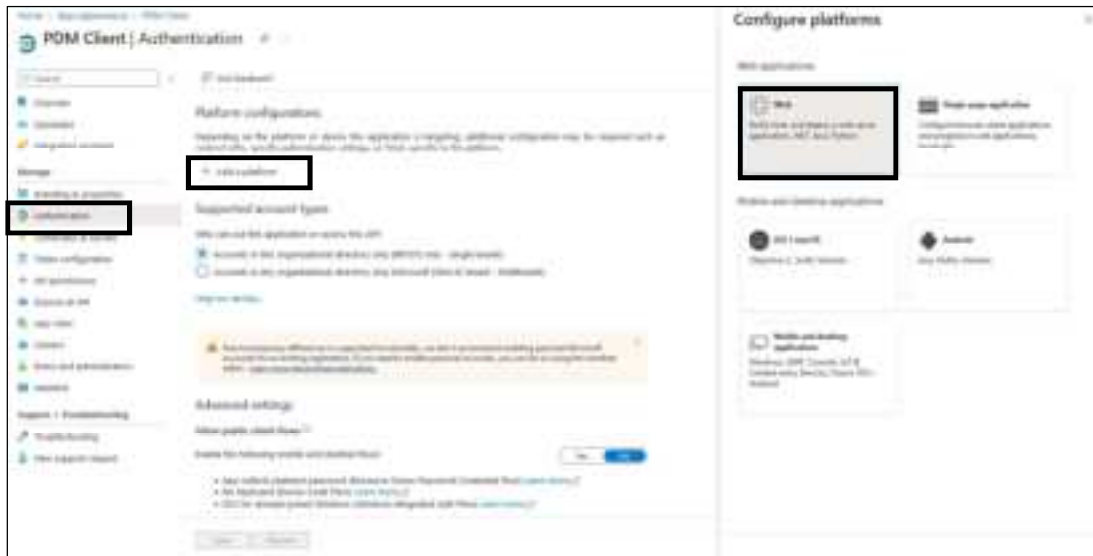
By proceeding, you agree to the Microsoft Platform Policies

Register

-
- The screenshot shows the PDM Client application interface. The left sidebar contains navigation links: Overview, Dashboard, Integration, Messages, and Settings. The main content area displays a list of applications. A red box highlights the 'Applications' section, which lists various applications with details like 'Application Name', 'Application ID', 'Application Type', 'Application Status', 'Application Version', and 'Application Description'. The 'Application Name' column is highlighted in blue.

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 –

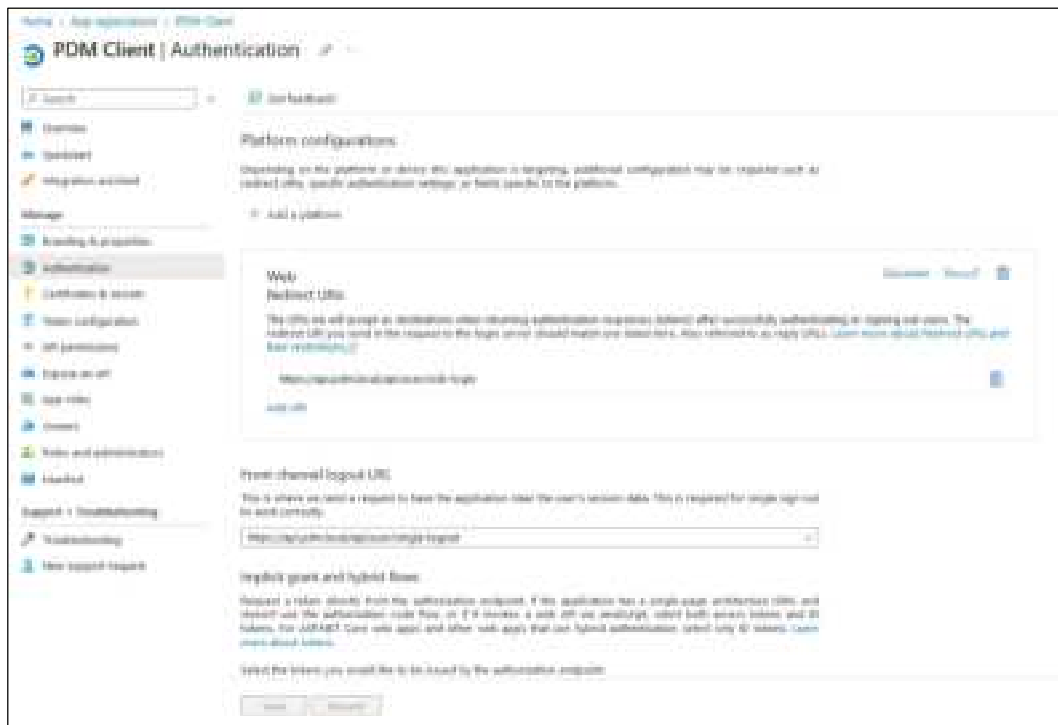
- (Optional) Enter the **Redirect URIs** - <https://api.pdm.local/api/user/oidc-login>
- Enter the **Front-channel logout URL** – PDM Front-channel Logout URI (<https://api.pdm.local/api/user/single-logout>). This field is needed only when implementing single sign on. **(Mandatory)**.

pdm.local - indicates the domain name.

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



→ The configuration details are displayed.

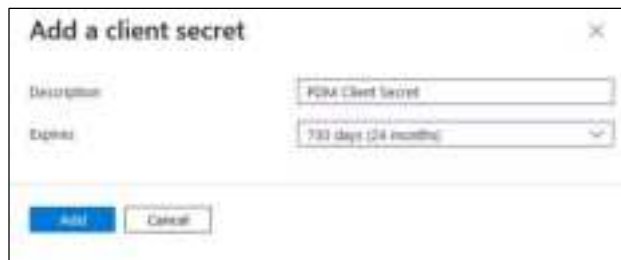


5.2.2.1.3 Setup Client Secret

→ 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.

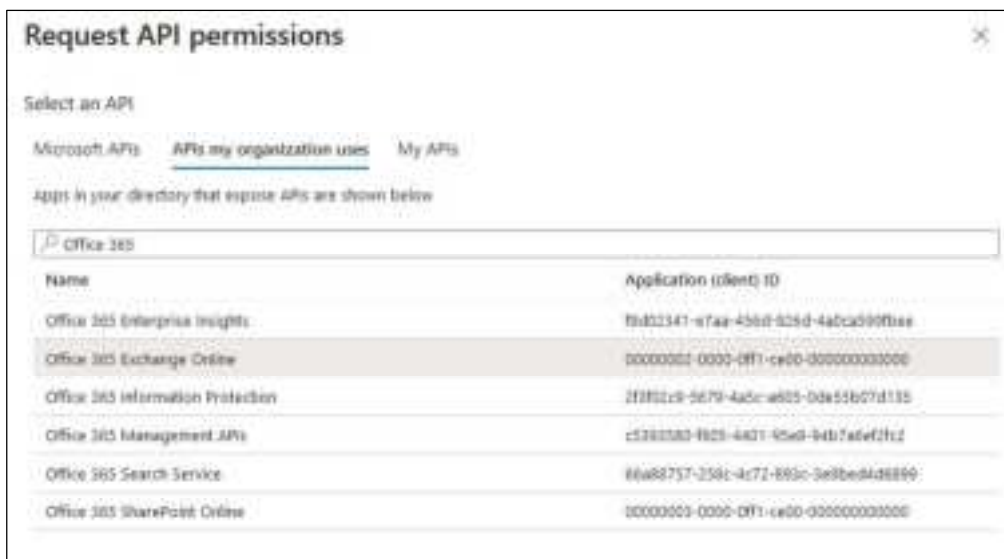


5.2.2.1.4 Setup API Permissions

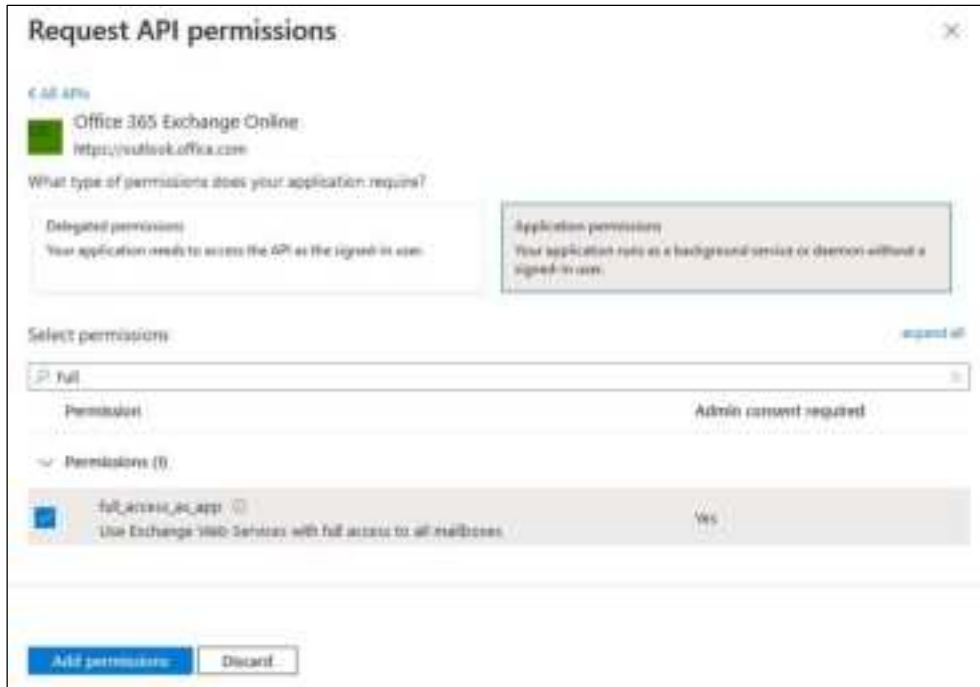
- From left navigation menu, go to **API permissions** → **Add a permission**.



- 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**.



Request API permissions

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](#)

Full

Permissions (1)

Permissions (1)	Admin consent required
full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes

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

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



PDM Client | API permissions

Search: Refresh: [Refresh](#) Test: [Test](#)

You are viewing permissions for your application. Open all items to see details if they are already done as permissions.

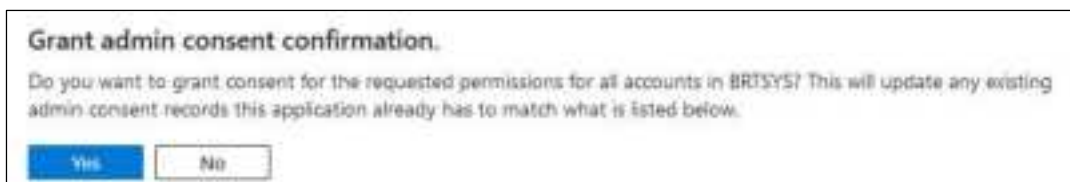
Configured permissions

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

[Add a permission](#) [Reset admin consent for all apps](#)

API / permission name	Type	Description	Admin consent req.	Status
Microsoft Graph (G)	Delegated	Sign in and read user profile	No	OK
Microsoft Exchange Online (G)	Delegated	Use Exchange Web Services with full access to all mailboxes	No	OK
Full access as app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	Not granted for BRTSYS

No view and manage consent permissions for individual apps, as well as your tenant's consent settings, by [Enterprise applications](#).

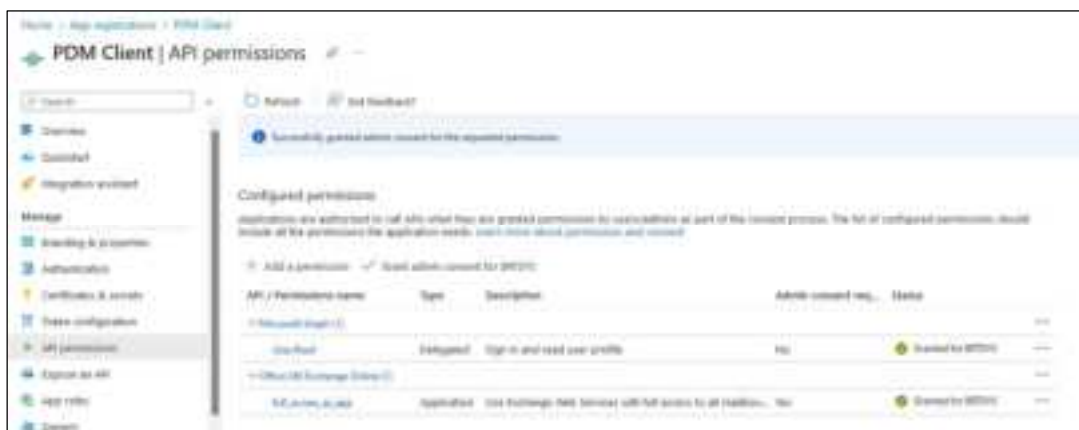


Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in BRTSYS? This will update any existing admin consent records this application already has to match what is listed below.

[Yes](#) [No](#)

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

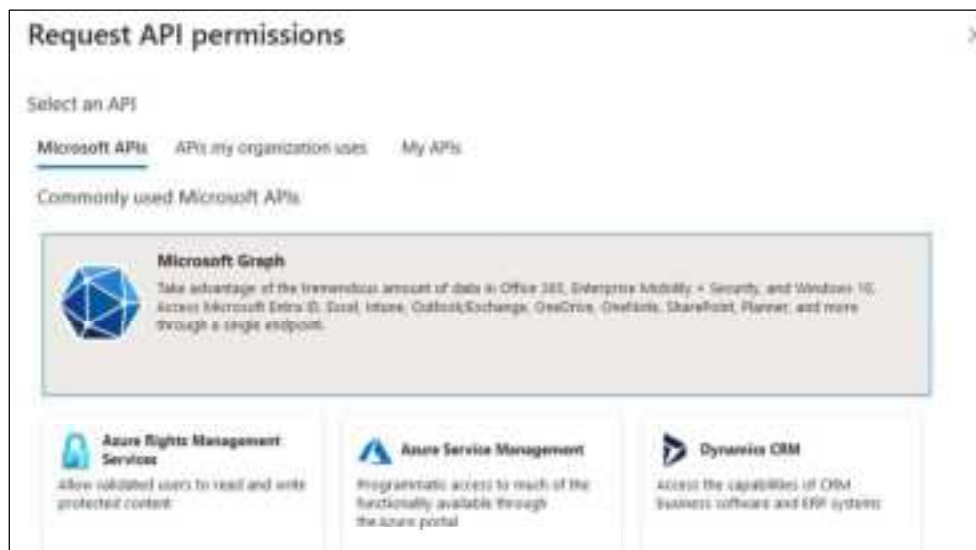


5.2.2.1.5 Setup Delegate Permissions

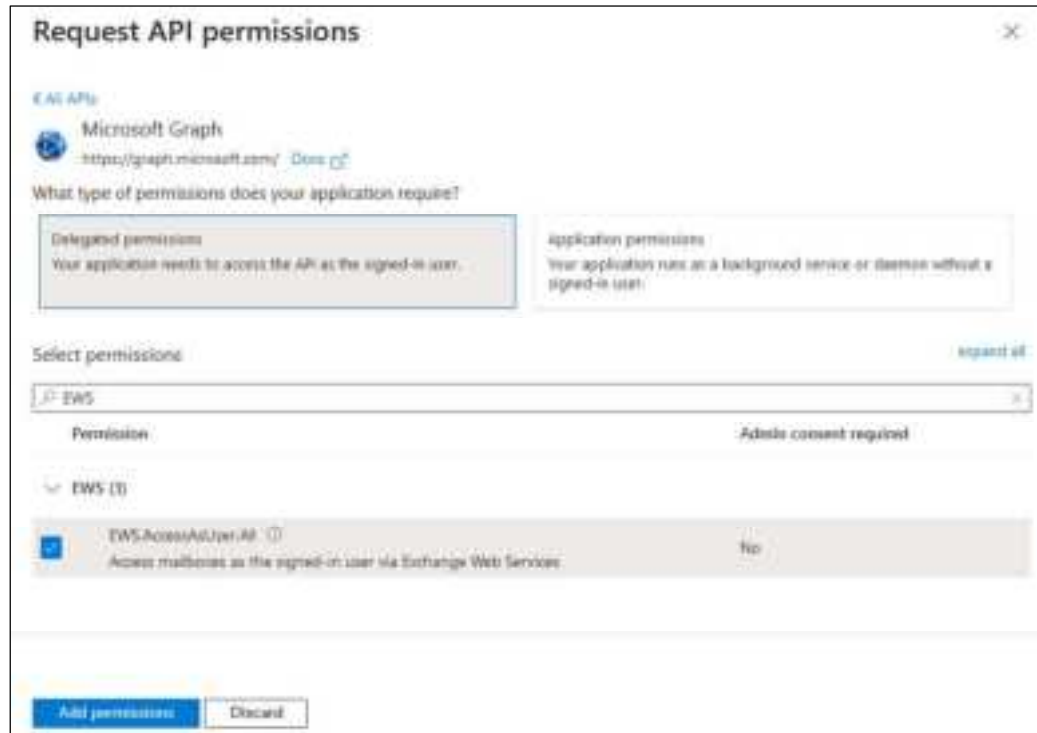
→ From left navigation menu, go to **API permissions** → **+ Add a permission**.



→ 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].



The dialog box is titled "Request API permissions" and shows the "EWS API" section. It includes the Microsoft Graph logo and URL. Under "What type of permissions does your application require?", the "Delegated permissions" option is selected. In the "Select permissions" section, "EWS" is chosen from the dropdown. The table below shows the selected permission:

Permission	Admin consent required
EWS (1)	
EWS.AccessAsUser.All (1)	No

Buttons at the bottom: "Add permissions" (blue) and "Discard" (grey).

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



The dialog box is titled "Request API permissions" and shows the "SMTP" section. Under "What type of permissions does your application require?", the "Delegated permissions" option is selected. In the "Select permissions" section, "SMTP" is chosen from the dropdown. The table below shows the selected permission:

Permission	Admin consent required
SMTP (1)	
SMTP.Send (1)	No

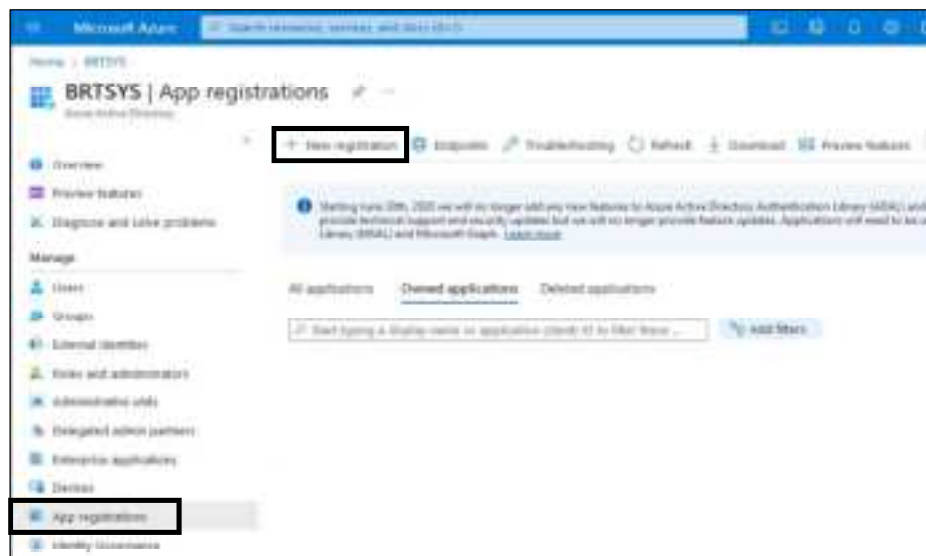
Buttons at the bottom: "Add permissions" (blue) and "Discard" (grey).

- 46

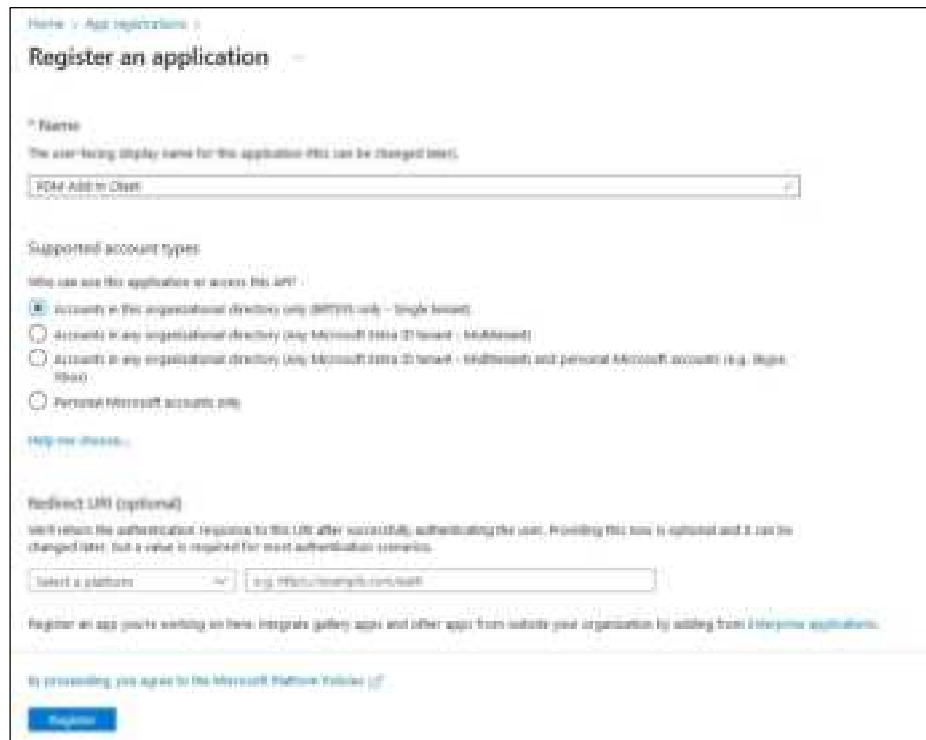
5.2.2.2 Add-In Client

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 –

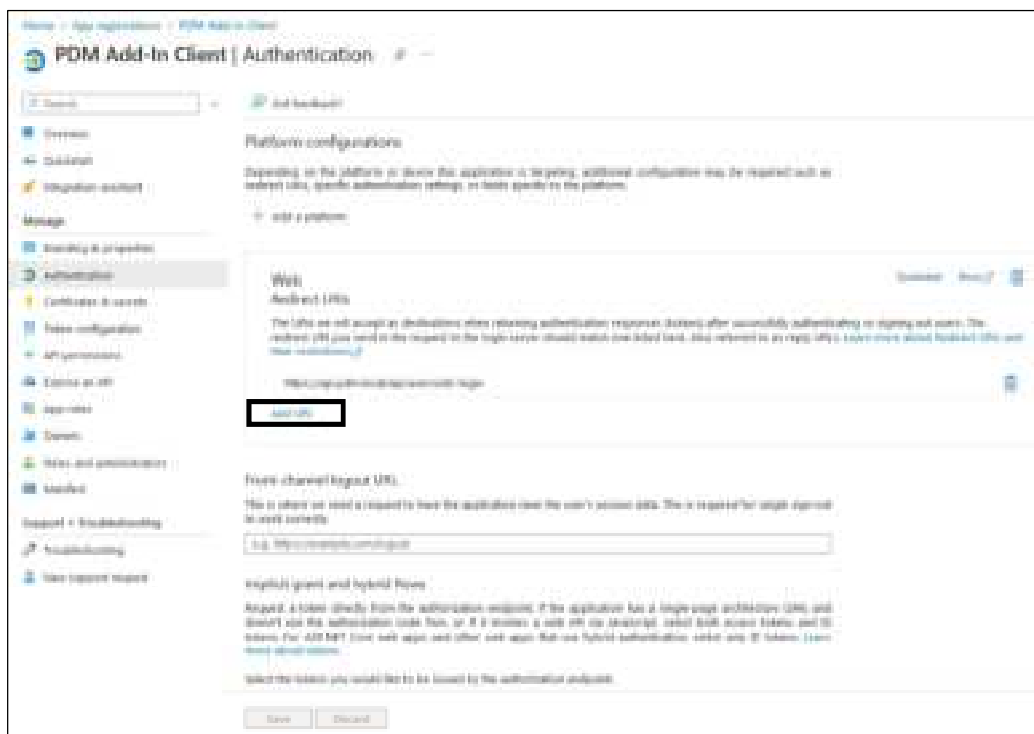
- Enter the **Redirect URIs** – PDM Login Redirect URI – For example, <https://api.pdm.local/api/user/oidc-login> (**Mandatory**).
- Enter the **Front-channel logout URL** - <https://api.pdm.local/api/user/single-logout>. This field is needed only when implementing single sign on. (Optional).

[pdm.local](https://api.pdm.local) - indicates the domain name.

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



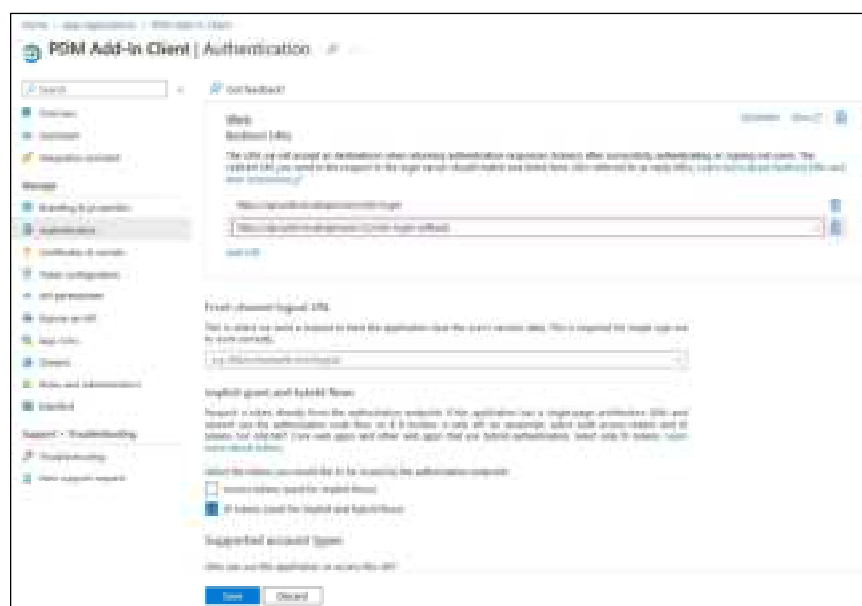
→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



The screenshot shows the 'PDM Add-In Client | Authentication' configuration page. The left sidebar contains a navigation menu with options like 'Overview', 'Configuration', 'Integration', 'Management', 'Reporting', 'Support', and 'Help'. The main content area is titled 'Platform configurations' and includes sections for 'Web Redirect URIs', 'Front-channel logout URL', and 'Implicit grant and hybrid flows'. The 'Web Redirect URIs' section has a text input field and a red box highlighting the 'Add URI' button.

→ 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



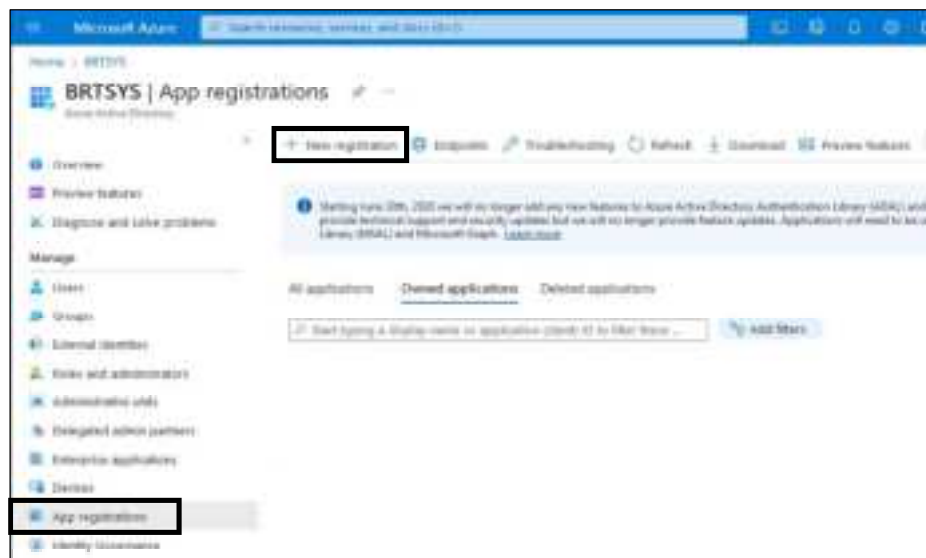
The screenshot shows the 'PDM Add-In Client | Authentication' configuration page. The left sidebar contains a navigation menu with options like 'Overview', 'Configuration', 'Integration', 'Management', 'Reporting', 'Support', and 'Help'. The main content area is titled 'Platform configurations' and includes sections for 'Web Redirect URIs', 'Front-channel logout URL', and 'Implicit grant and hybrid flows'. The 'Web Redirect URIs' section has a text input field and a red box highlighting the 'Add URI' button. The 'Front-channel logout URL' section has a text input field. The 'Implicit grant and hybrid flows' section has a checkbox for 'ID tokens' which is checked.

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

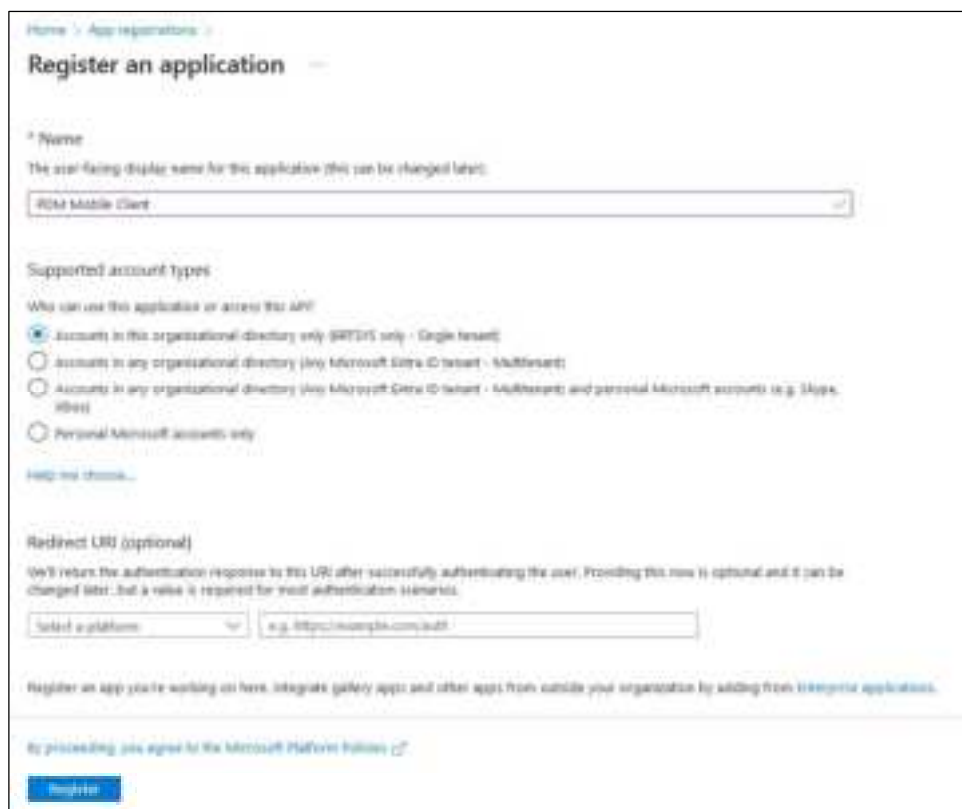
5.2.2.3 Mobile Client

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]**.



Home > App registrations > Register an application

Name

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

PDM Mobile Client

Supported account types

Who can use this application or access the API?

☒ Accounts in this organisational directory only (BRTSYS only - Single tenant)

☐ Accounts in any organisational directory (any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organisational 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.

Select a platform:

Register an app you're working on here. Integrate gallery apps and other apps from outside your organisation by adding from [Integrate applications](#).

By proceeding, you agree to the [Microsoft Platform Terms of Use](#).

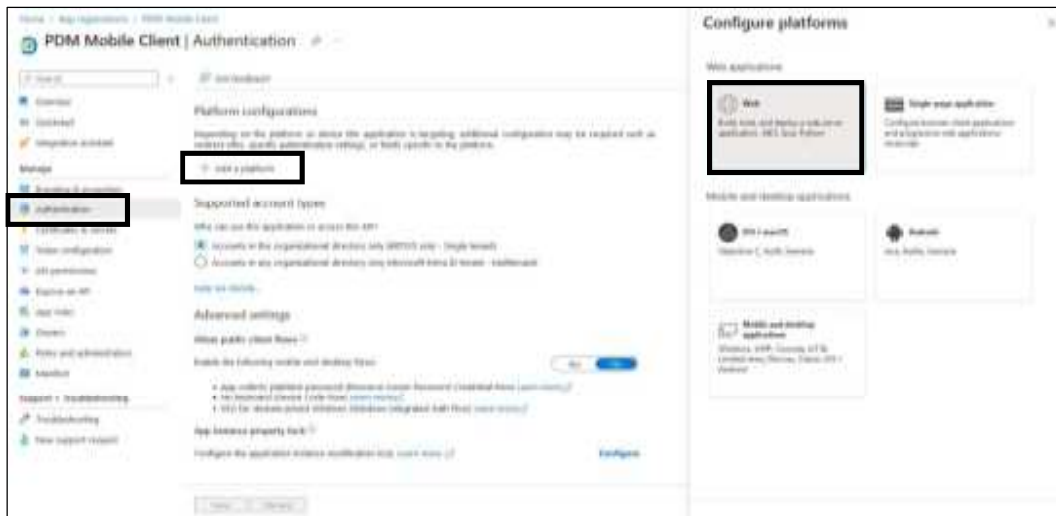
Register

→ 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 –

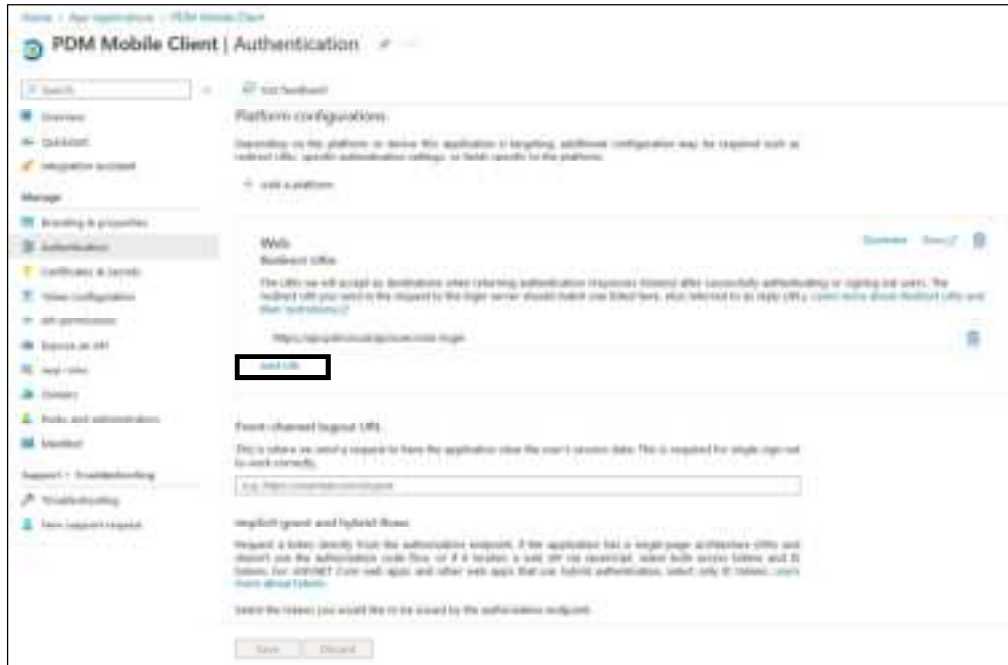
- Enter the **Redirect URIs** - PDM Login Redirect URI- For example, <https://api.pdm.local/api/user/oidc-login> (**Mandatory**).
- Enter the **Front-channel logout URL** - <https://api.pdm.local/api/user/single-logout>. This field is needed only when implementing single sign on. (Optional).

pdm.local - indicates the domain name.

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

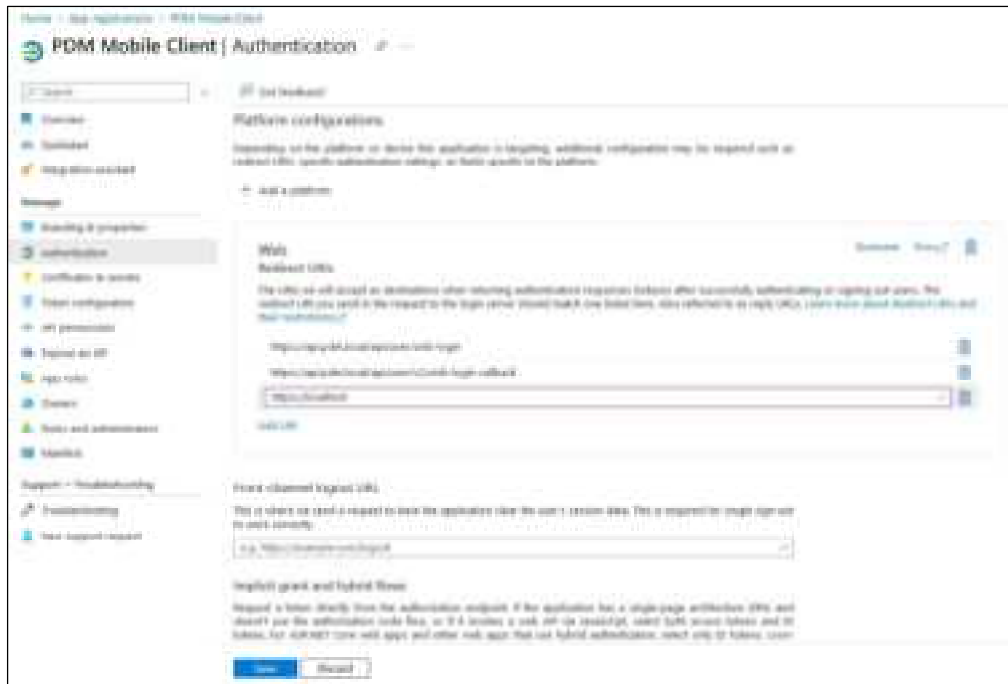


→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



→ 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]**.



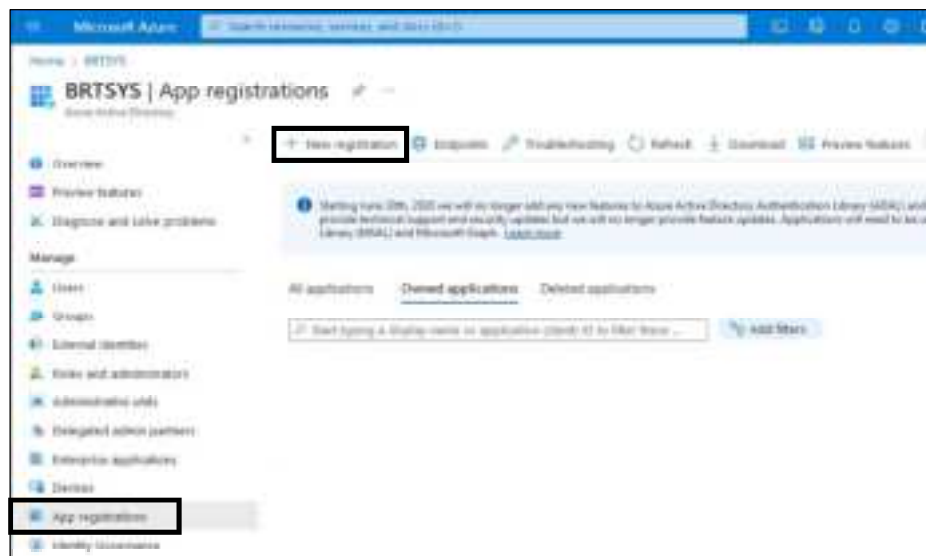
→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.



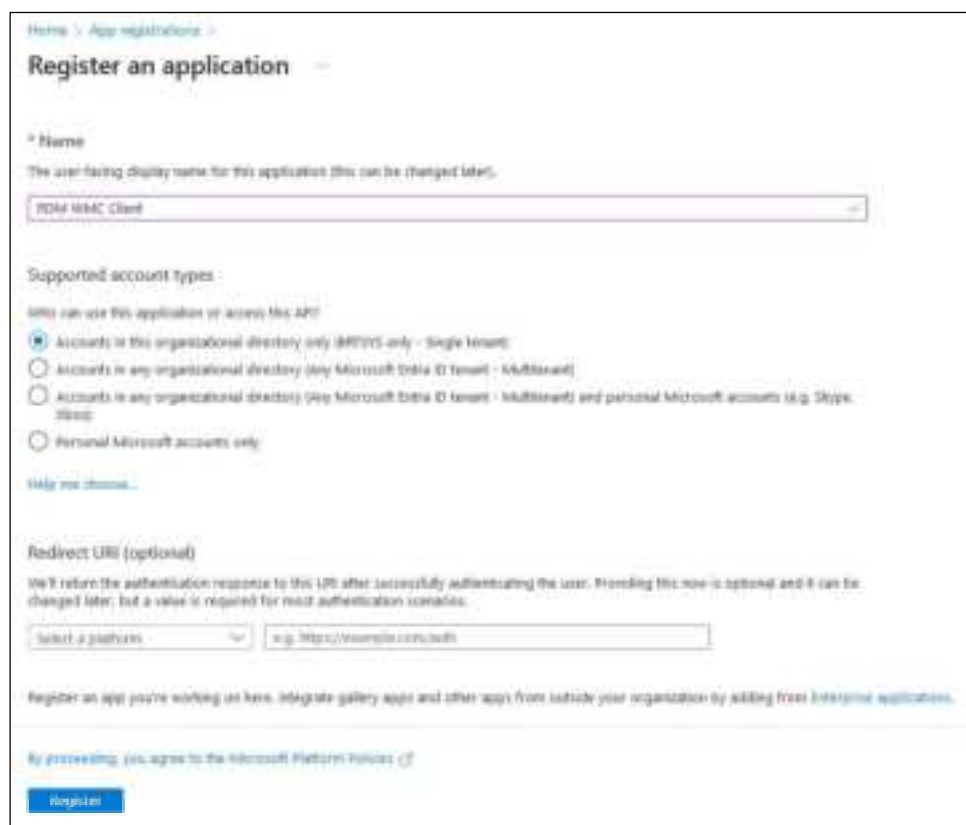
5.2.2.4 PDM Management Console (WMC Client)

5.2.2.4.1 App Registration

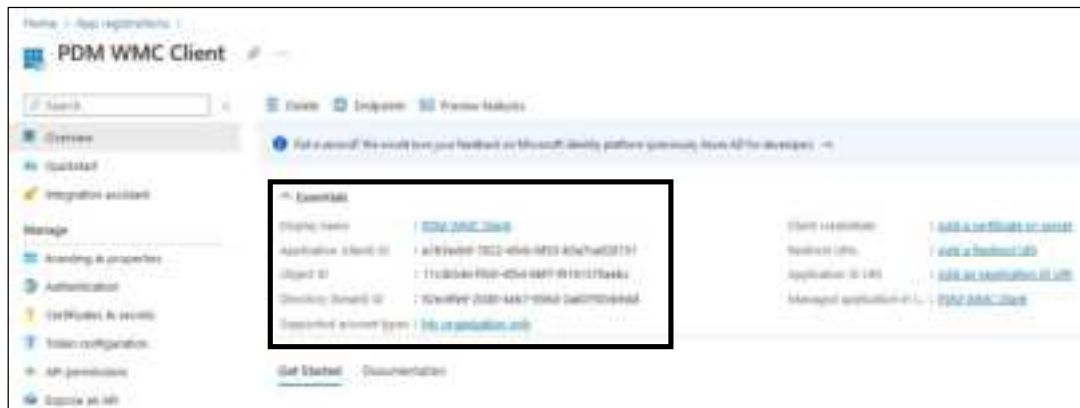
→ Select **App registrations**. Click **+ New registration**.



→ 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**.

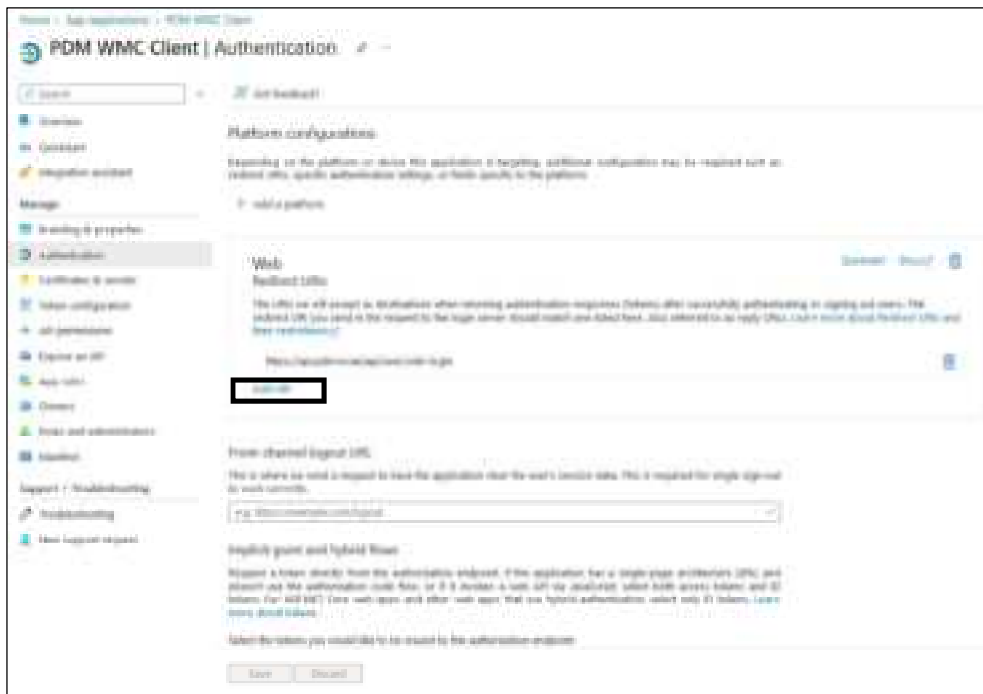


→ In the configure Web UI –

- 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](https://api.pdm.local) - indicates the domain name.
- Select **ID tokens** check box
- Click **[Configure]**.



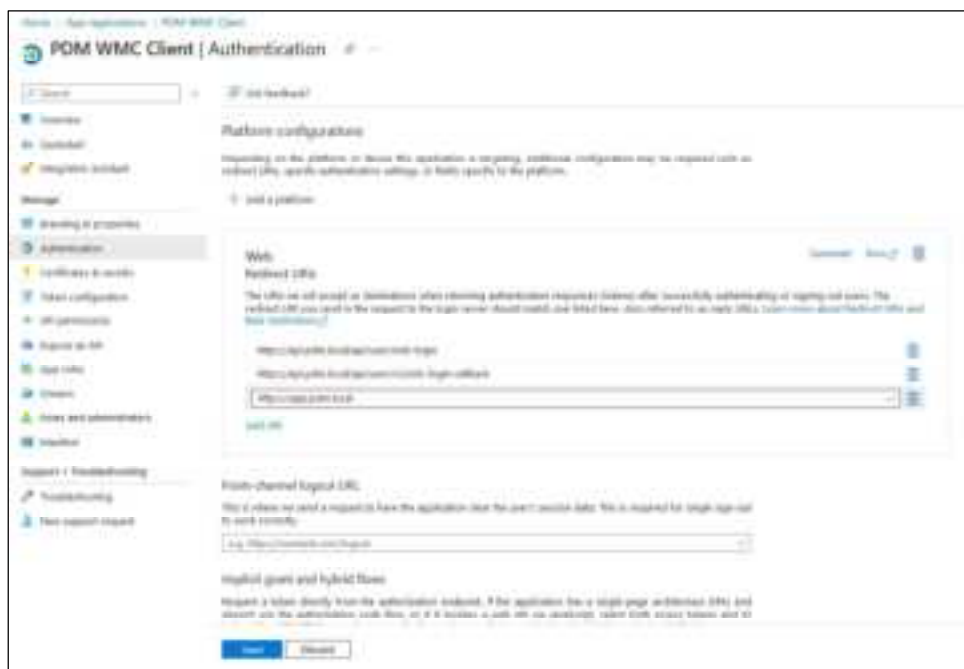
→ The configuration details are displayed. Click **[Add URI]** to additional Redirect URIs.



The screenshot shows the 'PDM WMC Client | Authentication' configuration page. The 'Web Redirect URI' field is highlighted with a red box. The page includes sections for 'Platform configurations', 'Web Redirect URI', 'Front-channel Logout URL', and 'Hybrid grant and hybrid flow'.

→ 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

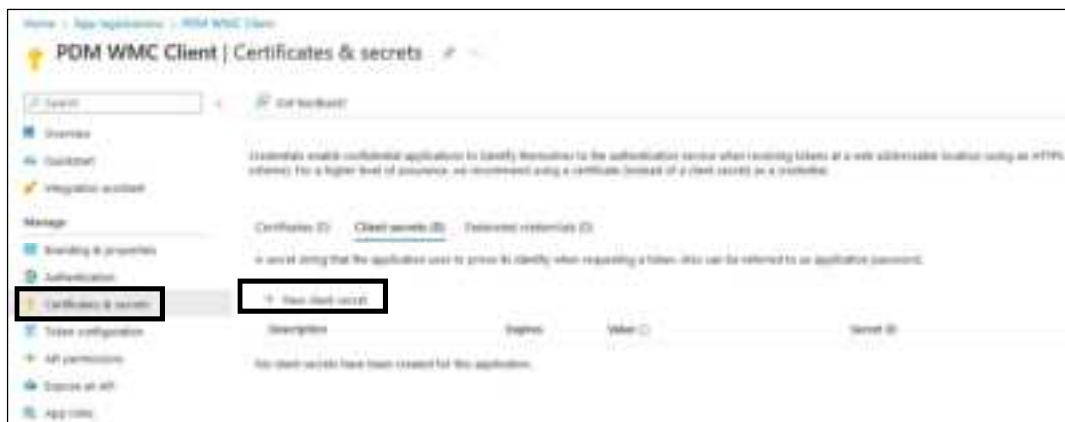


The screenshot shows the 'PDM WMC Client | Authentication' configuration page. The 'Web Redirect URI' field is highlighted with a red box. The page includes sections for 'Platform configurations', 'Web Redirect URI', 'Front-channel Logout URL', and 'Hybrid grant and hybrid flow'.

→ 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]**.

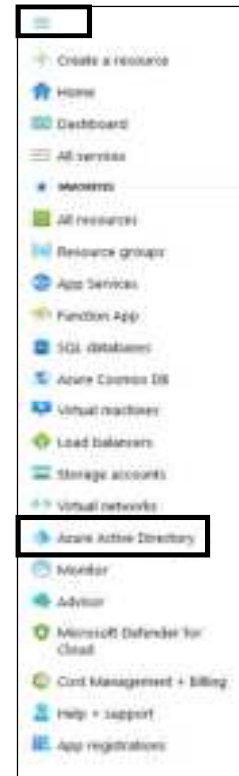


→ The newly created client secret's Value (not its Secret ID) should be copied and saved immediately. The value can no longer be viewed later.



5.2.3 Modern Authentication using OAuth 2.0 - ROPC

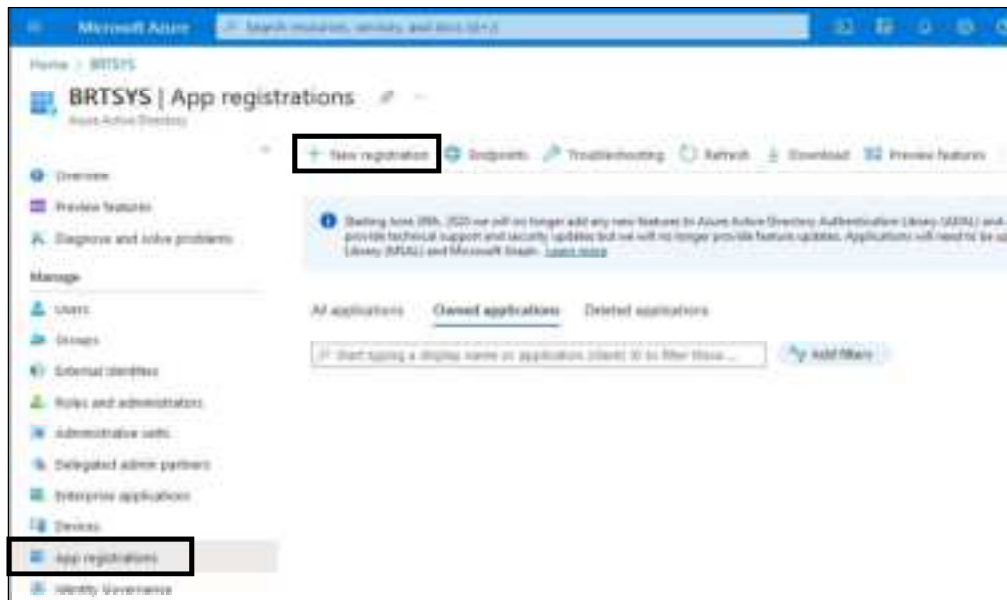
- Access Azure Portal using the administrator account – <https://portal.azure.com>.
- Go to **Azure Active Directory** from the left navigation menu.



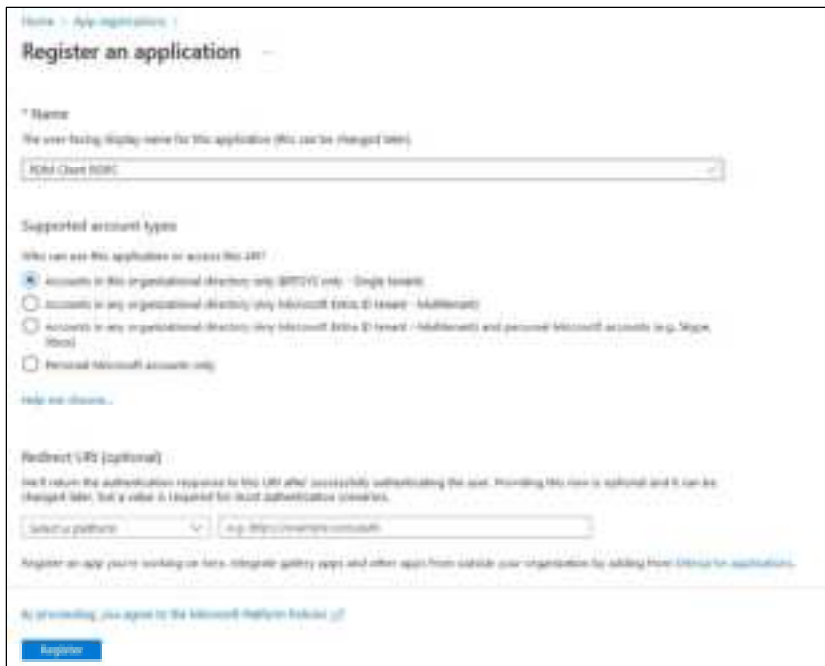
5.2.3.1 PDM Client

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]**.

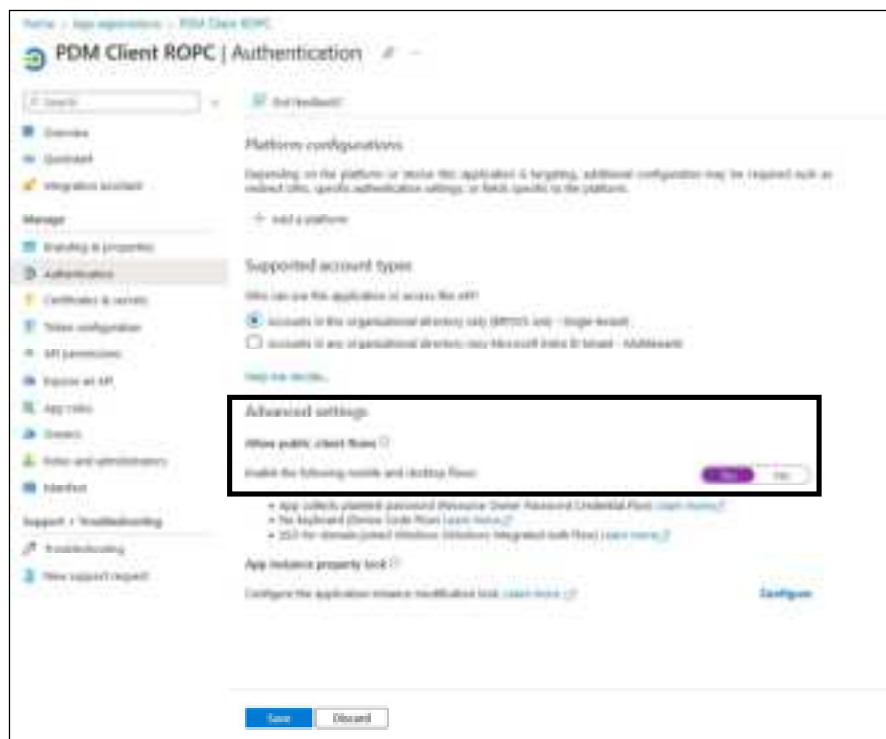


- The PDM Client ROPC application is successfully created.



5.2.3.1.2 Setup Authentication

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



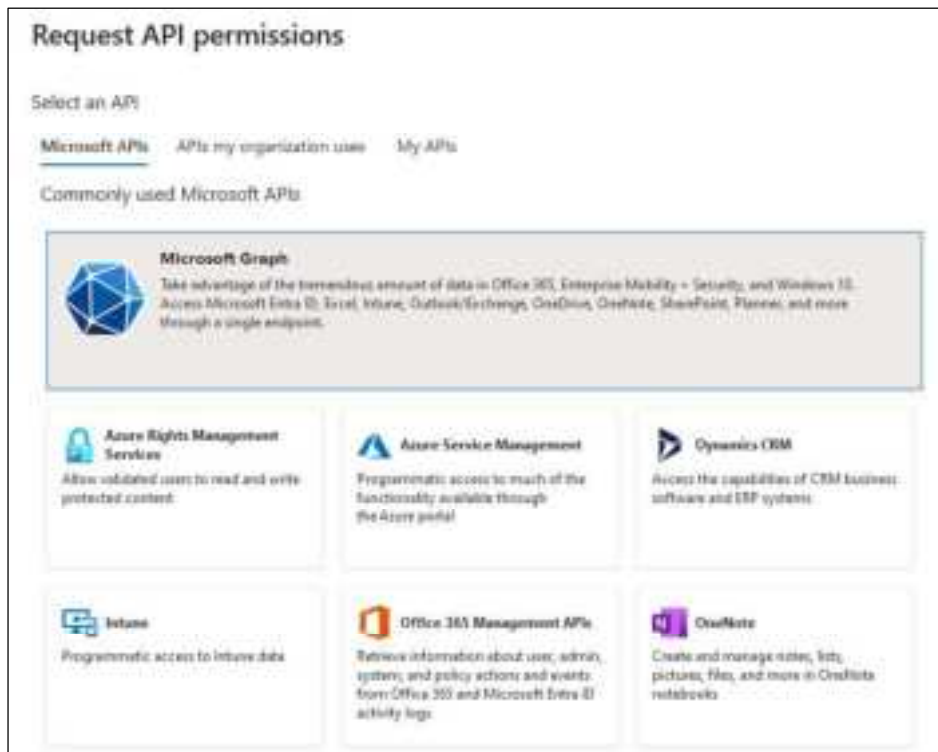
→ Click **[Save]**.

5.2.3.1.3 Setup API Permissions

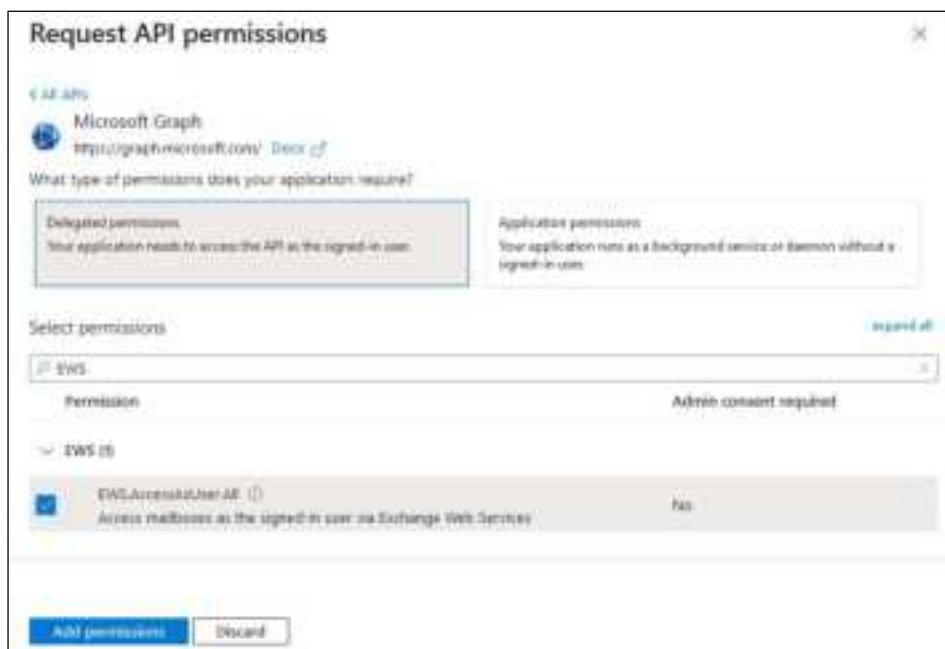
→ From left navigation menu, go to **API permissions** → **+ Add a permission**.



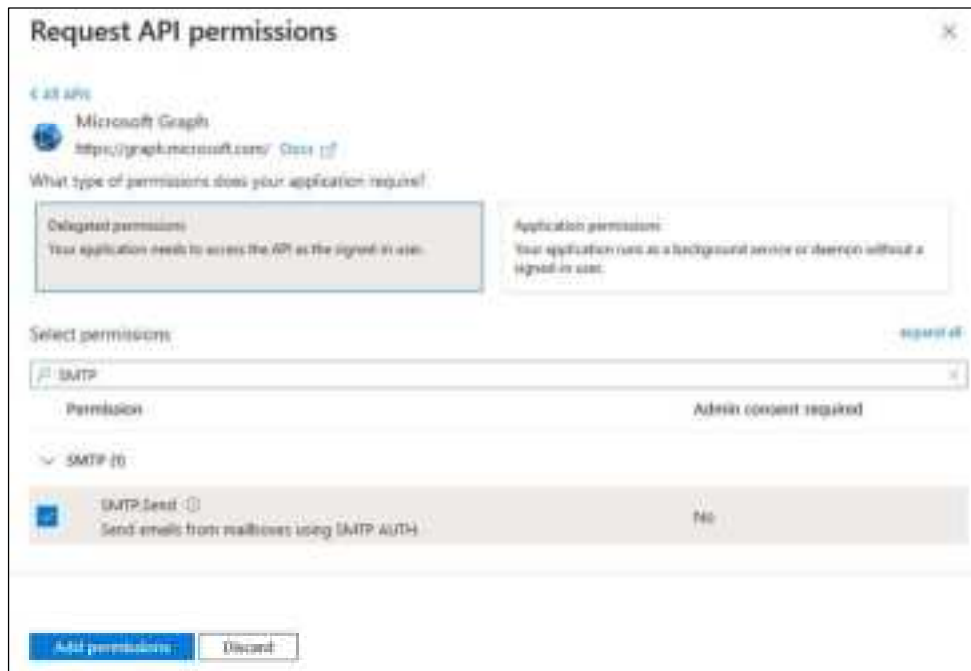
→ From the Request API permissions UI, click **Microsoft APIs** and select **Microsoft Graph**.



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



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



Request API permissions

← All APIs

Microsoft Graph
https://graph.microsoft.com/ Close

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

SMTP

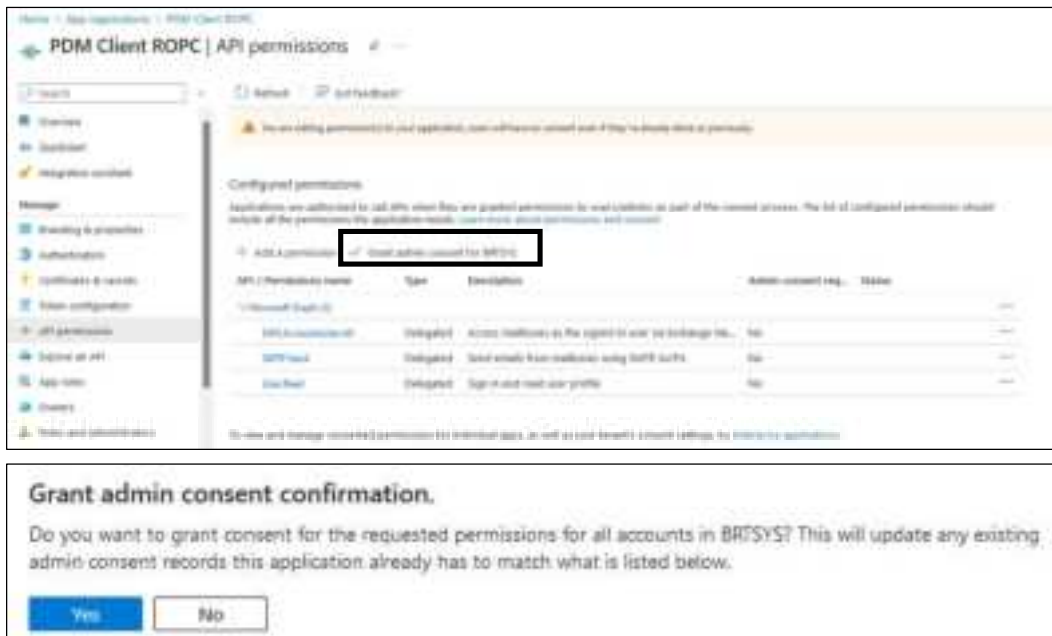
Permission Admin consent required

SMTP (0)

Permission	Admin consent required
SMTP.Send Send emails from mailboxes using SMTP AUTH	No

Add permissions **Discard**

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



Home > App registrations > PDM Client ROPC

PDM Client ROPC | API permissions

Search Add Remove Add Hybrid App

You are adding permissions to your application. You will have to grant admin consent if they're already listed at permission.

Configured permissions

Applications are authorized to call APIs when they are granted permissions to work on behalf of each of the consented users. The list of configured permissions should include all the permissions the application needs. You must grant permissions and consent.

ADD A PERMISSION **Grant admin consent for BRTSYS**

API (Permissions name)	Type	Description	Admin consent req.	Status
Microsoft Graph (0)				
API permissions (0)	Delegated	Access mailboxes as the signed-in user by delegating the...	No	On
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH	No	On
User.Read	Delegated	Sign and read user profile	No	On

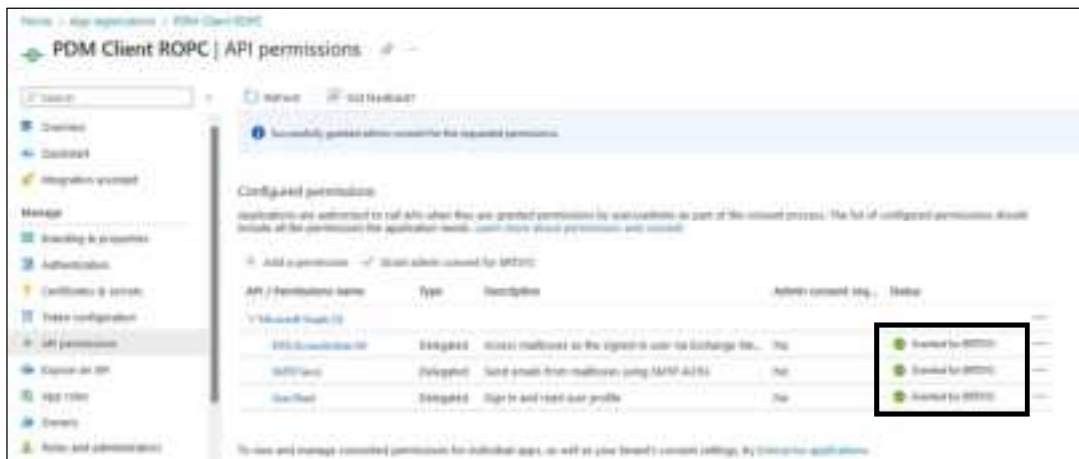
To view and manage assigned permissions for individual apps, as well as consent records and settings for interactive applications.

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in BRTSYS? This will update any existing admin consent records this application already has to match what is listed below.

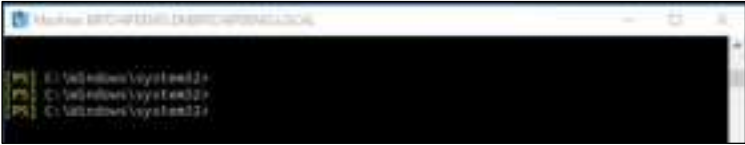
Yes **No**

→ 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 <i>Exchange Management Shell</i> is opened. 
→ Create User Account	c. Create user account using the following command – <pre>New-Mailbox -Name "User1" -DisplayName "User1" - UserPrincipalName "user1@bridgetek.com" - OrganizationalUnit Users -Password (ConvertTo- SecureString "P@ssw0rd" -AsPlainText -force)</pre>
→ 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 <i>RoomList</i> parameter as it is not required. d. Create a new user distribution group named "<i>pdm-user-group- <groupname></i>" using the following command – <pre>New-DistributionGroup -Name "pdm-user-group- bridgetek1"</pre>
	Note: A distribution group name should begin with prefix <i>pdm-user-group</i> and be followed by the group name.
	e. Add a user account (user1@bridgetek.com) to an existing user distribution group list (<i>pdm-user-group-bridgetek1</i>) using the following command – <pre>Add-DistributionGroupMember -Identity "pdm-user- group-bridgetek1" -Member user1@bridgetek.com</pre> f. Use the following command to display a list of users who have been added to a particular distribution group – <pre>Get-DistributionGroupMember -Identity "pdm-user- group-bridgetek1"</pre>
→ Create Desk / Resource Account	g. Using the following command, create a resource account – <pre>New-Mailbox -Name "Desk1" -DisplayName "Desk1" -Room</pre>
→ 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 <i>RoomList</i> parameter as it is not required.

	h. Create a new desk distribution group named "<i>pdm-desk-group- <groupname></i>" using the following command - <pre>New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList</pre>
	Note: A distribution group name should begin with prefix <i>pdm-desk-group</i> and be followed by the group name.
	i. Add a resource account (<i>desk1@bridgetek.com</i>) to an existing desk list (<i>pdm-desk-group-bridgetek1</i>) using the following command - <pre>Add-DistributionGroupMember -Identity "pdm-desk-group-bridgetek1" -Member desk1@bridgetek.com</pre> j. Use the following command to display a list of desks that have been added to a particular distribution group - <pre>Get-DistributionGroupMember -Identity " pdm-desk-group-bridgetek1"</pre>
→ Create Impersonation User / Service Account	k. Create Service Account using the following command - <pre>New-Mailbox -Name "service-account" -DisplayName "service-account" -UserPrincipalName "service-account@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)</pre>
→ Grant Service Account Impersonation Rights	l. Create Admin Role Group and Grant Service Account Impersonation Rights using the following command - <pre>New-RoleGroup -Name "Application Impersonation Role" -Roles "ApplicationImpersonation" -Members service-account@bridgetek.com</pre> m. Using the following command, view the application impersonation data - <pre>Get-ManagementRoleAssignment -Role "ApplicationImpersonation" -GetEffectiveUsers</pre>
→ Discovery Management	n. Using the following command, add the service account into Discovery Management Role - <pre>Add-RoleGroupMember -Identity "Discovery Management" -Member service-account@bridgetek.com</pre> o. View the list of members in the Discovery Management Role, using the following command - <pre>Get-RoleGroupMember -Identity "Discovery Management"</pre>

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. <pre>\$Install-Module-Name ExchangeOnlineManagement</pre> c. Using the following command, import the Exchange Online Management Module – <pre>\$ Import-Module ExchangeOnlineManagement</pre> d. Using the following command connect to the Exchange Online Management Module. <pre>Connect-ExchangeOnline -UserPrincipalName Administrator@bridgetek.com</pre> Now the Microsoft 365 can be managed via PowerShell.
→ Create User Account	e. Create user account using the following command – <pre>New-Mailbox -Name "User1" -DisplayName "User1" -UserPrincipalName "user1@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)</pre>
→ 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 <i>RoomList</i> parameter as it is not required. e. Create a new user distribution group named "<i>pdm-user-group-<groupname></i>" using the following command – <pre>New-DistributionGroup -Name "pdm-user-group-bridgetek1"</pre>
	Note: A distribution group name should begin with prefix <i>pdm-user-group</i> and be followed by the group name.
	f. Add a user account (<i>user1@bridgetek.com</i>) to an existing user distribution group list (<i>pdm-user-group-bridgetek1</i>) using the following command – <pre>Add-DistributionGroupMember -Identity "pdm-user-group-bridgetek1" -Member user1@bridgetek.com</pre> g. Use the following command to display a list of users who have been added to a particular distribution group – <pre>Get-DistributionGroupMember -Identity "pdm-user-group-bridgetek1"</pre>
→ Create Desk / Resource Account	h. Using the following command, create a resource account – <pre>New-Mailbox -Name "Desk1" -DisplayName "Desk1" -Room</pre>

→ 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 <i>RoomList</i> parameter as it is not required. i. Create a new desk distribution group named "<i>pdm-desk-group-<groupname></i>" using the following command - <pre>New-DistributionGroup -Name "pdm-desk-group-bridgetek1" -RoomList</pre>
	Note: A distribution group name should begin with prefix <i>pdm-desk-group</i> and be followed by the group name.
	j. Add a resource account (desk1@bridgetek.com) to an existing desk list (<i>pdm-desk-group-bridgetek1</i>) using the following command - <pre>Add-DistributionGroupMember -Identity "pdm-desk-group-bridgetek1" -Member desk1@bridgetek.com</pre> k. Use the following command to display a list of desks that have been added to a particular distribution group - <pre>Get-DistributionGroupMember -Identity "pdm-desk-group-bridgetek1"</pre>
→ Create Impersonation User / Service Account	l. Create Service Account using the following command - <pre>New-Mailbox -Name "service-account" -DisplayName "service-account" -UserPrincipalName "service-account@bridgetek.com" -OrganizationalUnit Users -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force)</pre>
→ Grant Service Account Impersonation Rights	m. Create Admin Role Group and Grant Service Account Impersonation Rights using the following command - <pre>New-RoleGroup -Name "Application Impersonation Role" -Roles "ApplicationImpersonation" -Members service-account@bridgetek.com</pre> n. Using the following command, view the application impersonation data - <pre>Get-ManagementRoleAssignment -Role "ApplicationImpersonation" -GetEffectiveUsers</pre>
→ Discovery Management	o. Using the following command, add the service account into Discovery Management Role - <pre>Add-RoleGroupMember -Identity "Discovery Management" -Member service-account@bridgetek.com</pre> p. View the list of members in the Discovery Management Role, using the following command - <pre>Get-RoleGroupMember -Identity "Discovery Management"</pre>

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

Table 1 - Hardware / Software Requirements	5
Table 2 – Network Port Requirements	5

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