

USER GUIDE

P2NL

Desk Manager 3.1.0

Part 2 – Installation and Configuration



Document Version: 2.0

Issue Date: 01-07-2024

Neither the whole nor any part of the information contained in, or the product described in this manual may be adapted or reproduced in any material or electronic form without the prior written consent of the copyright holder. This product and its documentation are supplied on an as-is basis and no warranty as to their suitability for any particular purpose is either made or implied. BRT Systems Pte Ltd will not accept any claim for damages howsoever arising as a result of use or failure of this product. Your statutory rights are not affected. This product or any variant of it is not intended for use in any medical appliance device or system in which the failure of the product might reasonably be expected to result in personal injury. This document provides preliminary information that may be subject to change without notice. No freedom to use patents or other intellectual property rights is implied by the publication of this document.



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		
Network Ports	Exchange Server	Port 443 Port 587	Used for EWS connection 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.

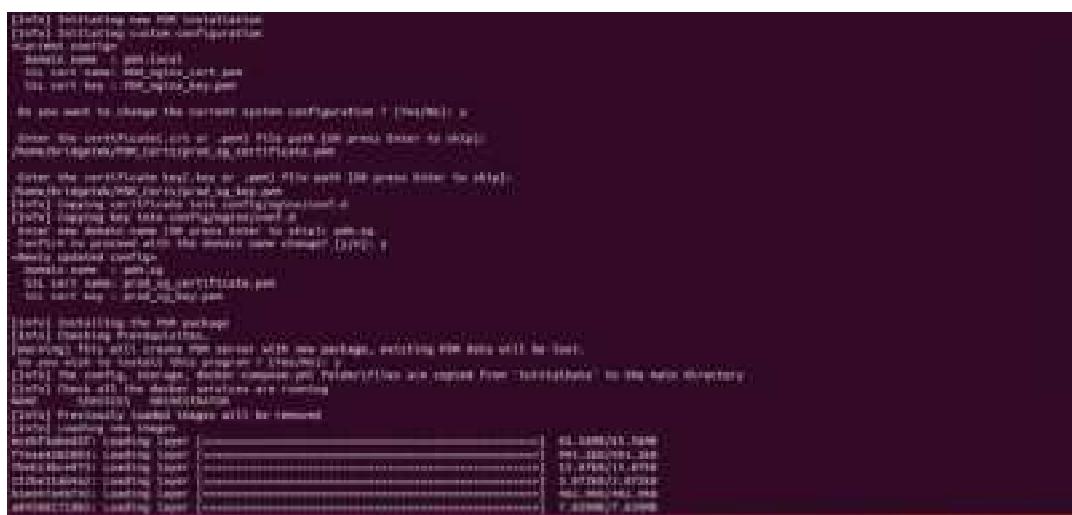
- Open a terminal / command prompt from the package directory (*for example - PDM_package_3.0.0-2.1.0-P*) and enter the following command to provide the execution permission for the script files.

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

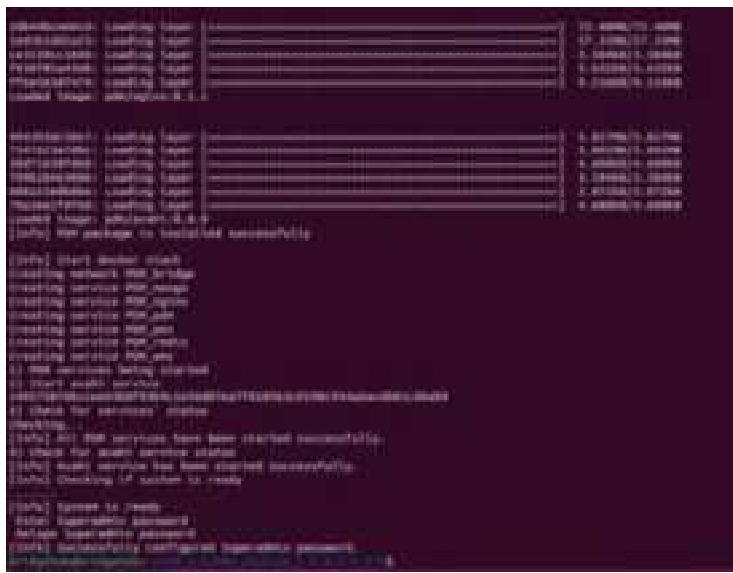
- Run the following command to install the software -

```
$ 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>

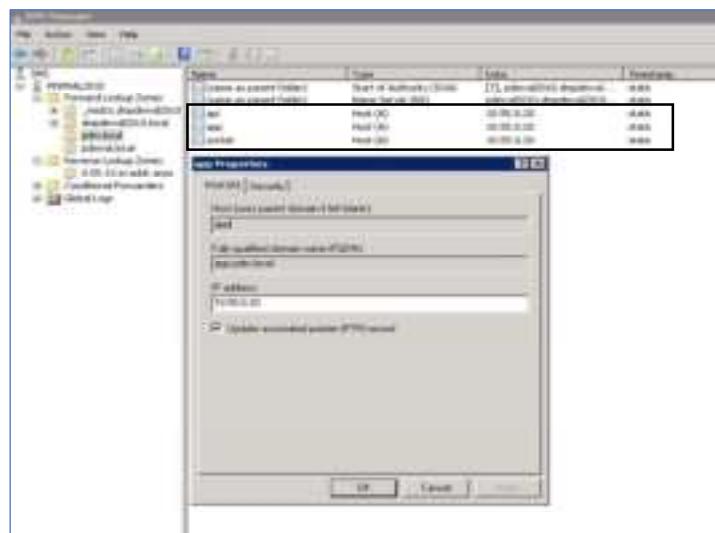
where in the *domain name* refers to the *organization's domain name*. For example, if the organization's name is ABC Pte Ltd, then the domain name can be abc.com or abc.local.

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-

A screenshot of the GoDaddy DNS Management interface. The top navigation bar includes 'GoDaddy', 'Domains', 'Buy & Sell', 'DNS', 'Settings', and 'Help'. Below the navigation is a search bar with placeholder 'Search' and a dropdown menu with 'My Domains'. The main title 'DNS Management' is centered above a table. The table has a header row 'Records' and columns 'Type', 'Name', 'Value', and 'TTL'. There are three entries: one 'A' record pointing to 'www' with a TTL of 1 hour, another 'A' record pointing to 'www' with a TTL of 4 hours, and a third 'A' record pointing to 'www' with a TTL of 1 day. Each entry has a pencil icon to its right.



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 – <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 – <ul style="list-style-type: none"> • 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 -> System</i>”.

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



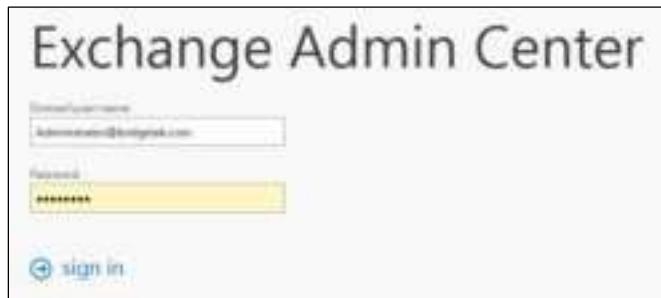
Note: Refer to the steps given under [Appendix > Exchange Server setup using Exchange Management Shell – Quick Reference](#) for more details.

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.

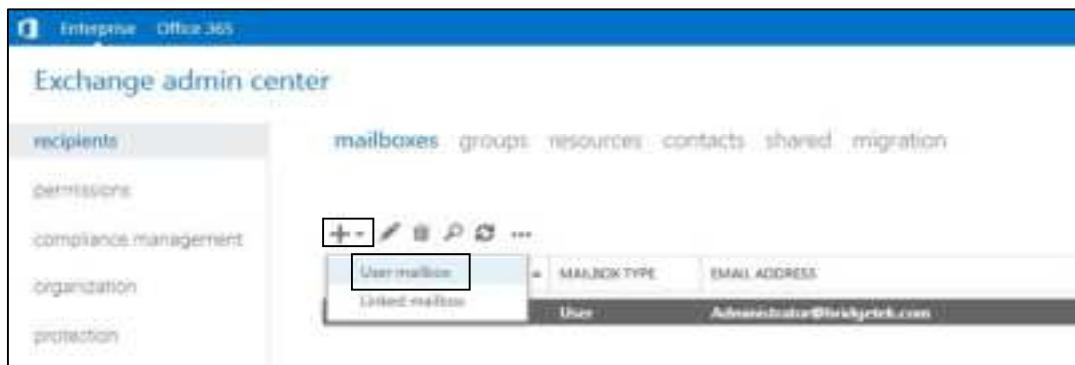


→ **Create User Account**

- Go to “**recipients**” → “**mailboxes**”.



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



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

The screenshot shows the 'new user mailbox' configuration dialog box. The 'Alias' field contains 'User1'. The 'User type' section has 'Existing user' selected. Below it, 'First name' is set to 'User1', 'Initials' to 'U', 'Last name' to 'User1', and 'Display name' to 'User1'. Under 'Name', 'User1' is listed. The 'Organizational unit' field has 'Browse...' selected. In the 'User logon name' field, 'user1' is entered, followed by '@' and 'bridgeTek.com'. The 'Email address' field shows 'user1@bridgeTek.com'. At the bottom, the 'Save' button is highlighted.

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

The screenshot shows the Exchange admin center interface. On the left, there's a navigation menu with 'recipients' selected. The main area displays a table of mailboxes. The first row shows 'Administrator' as the display name, 'User' as the mailbox type, and 'Administrator@bridgeTek.com' as the email address. The second row, which is highlighted, shows 'user1' as the display name, 'User' as the mailbox type, and 'user1@bridgeTek.com' as the email address.

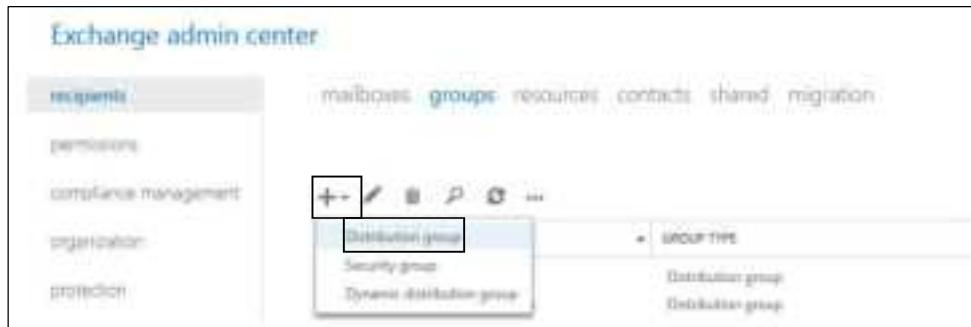
→ Create Distribution Group for Users

- Go to "recipients" → "groups".

The screenshot shows the Exchange admin center interface again. This time, the 'groups' tab is selected in the top navigation bar. The left sidebar still shows 'recipients' as the active category.



- Click “+” and select “**Distribution group**”.



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

new distribution group

Display name: pdm-user-group-bridge@t1
Notes: pdm-user-group-bridge@t1

Organizational unit:

Owners:
+ - **Administrator**

Members:
 Add group owners as members
+ -

Choose whether anyone can 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 owner. All requests to join will be rejected automatically.
 Owner approval: All requests are approved or rejected by the group owner.

- The newly added distribution group is displayed.

The screenshot shows the Exchange admin center interface. The left sidebar has 'recipients' selected. The top navigation bar includes 'mailboxes', 'groups', 'resources', 'contacts', 'shared', and 'migration'. Below the navigation is a toolbar with icons for '+', search, and other actions. A table lists recipients with columns for 'DISPLAY NAME', 'GROUP TYPE', and 'EMAIL ADDRESS'. The last entry is 'pdm user group-faqgroup1@...', which is highlighted.

→ Create Desk / Resource Account

- In the Exchange admin centre go to “recipients” → “resources”.

The screenshot shows the Exchange admin center interface with 'resources' selected in the left sidebar. The top navigation bar includes 'mailboxes', 'groups', 'resources', 'contacts', 'shared', and 'migration'. Below the navigation is a toolbar with icons for '+', search, and other actions. A table lists resources with columns for 'DISPLAY NAME', 'MAILBOX TYPE', and 'EMAIL ADDRESS'. A message at the bottom states: 'There are no items to show in this view.'

- Click “+” and select “Room mailbox”.

The screenshot shows the Exchange admin center interface with 'recipients' selected in the left sidebar. The top navigation bar includes 'mailboxes', 'groups', 'resources', 'contacts', 'shared', and 'migration'. Below the navigation is a toolbar with icons for '+', search, and other actions. A table lists mailbox types with columns for 'DISPLAY NAME', 'MAILBOX TYPE', and 'EMAIL ADDRESS'. The 'Room mailbox' option is highlighted under the '+' button. A message at the bottom states: 'There are no items to show in this view.'

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

A room mailbox is a resource mailbox that's assigned to a physical location. Users can easily request rooms by including room mailboxes in meeting requests. Just select the room mailbox from the list and add properties such as hosting requests or mailbox delegation, if required.

Room name: Desk1

Name: Desk1

Organizational Unit: Browse...

Location: S0-07-B8

Phone:

Capacity: 1

Save Cancel

- 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”.

The screenshot shows the Exchange admin center interface. The left sidebar has tabs for recipients, permissions, compliance management, organization, and protection. The main area has tabs for mailboxes, groups, resources, contacts, shared, and migration. Under the mailboxes tab, there is a list of mailboxes. One entry is highlighted: "User1" with a display name of "Administrator", a mail type of "User", and an email address of "Administrator@bridgeit.com".

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

The screenshot shows the Exchange admin center interface. The left sidebar has tabs for recipients, permissions, compliance management, organization, and protection. The main area has tabs for mailboxes, groups, resources, contacts, shared, and migration. A dropdown menu is open next to the "+" button, and the "User mailbox" option is highlighted. Below the dropdown, a table lists existing mailboxes: "User1" (display name "Administrator", mail type "User", email address "Administrator@bridgeit.com").

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

The screenshot shows the "new user mailbox" dialog box. It has sections for "Basic" and "Optional". In the "Basic" section, "Service account" is set to "service-account" and "Display name" is "service-account". In the "Optional" section, "Service account name" is "service-account", "Service account password" is "password", and "Confirm password" is "password". At the bottom are "Save" and "Cancel" buttons.



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

The screenshot shows the Exchange admin center interface. On the left, there's a sidebar with links: recipients, permissions (which is selected), compliance management, organization, protection, and mail flow. The main area is titled 'Exchange admin center' and shows a table of mailboxes. The table has columns for DISPLAY NAME, MAILBOX TYPE, and EMAIL ADDRESS. It lists three accounts: 'Administrator' (User, administrator@bridgeit.com), 'User1' (User, user1@bridgeit.com), and 'service-account' (User, service-account@bridgeit.com). The 'service-account' row is highlighted with a dark grey background.

→ 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 “**+**”.

The screenshot shows the Exchange admin center with the 'permissions' link selected in the sidebar. The main area is titled 'Exchange admin center' and shows a table for 'admin roles'. The table has columns for NAME and other details. A '+' button is visible at the top right of the table area. The 'permissions' link in the sidebar is highlighted with a black box.

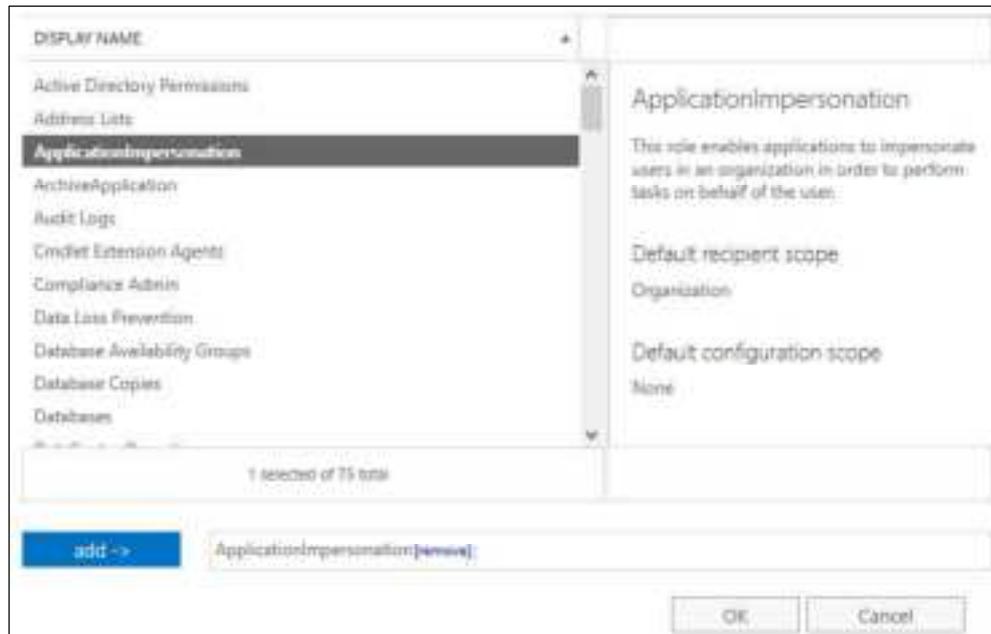
- Input the role group related details. Set the “*Write scope*” field as **Default** (for all accounts).

The screenshot shows a 'new role group' configuration dialog box. It has fields for 'Name' (set to 'Application Impersonation Role'), 'Description' (empty), and 'Write scope' (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**”.

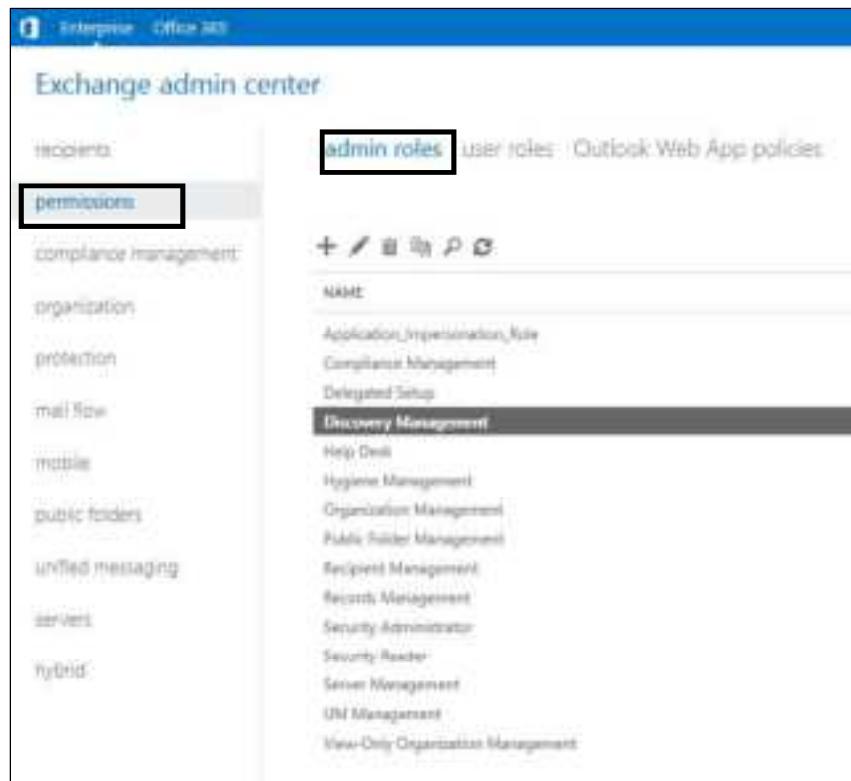
A screenshot of a software interface showing the 'admin roles' list. On the left is a sidebar with various management options like Compliance Management, Delegated Setup, Discovery Management, Help Desk, App Item Management, Organization Management, Public Folder Management, Recipient Management, Records Management, Security Administrator, Security Reader, Service Management, Site Management, View Only Organization Management, and View Only Organization Management. On the right, a detailed view of the 'Application Impersonation Role' is shown, including its assigned role, members, managed by, and write scope.



→ 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: [empty]

Role: + -

NAME	DISPLAY NAME
Legal Hold	Legal Hold
Mailbox Search	Mailbox Search
MailboxSearchApplication	MailboxSearchApplication

Members: + -

NAME	DISPLAY NAME
pm-admin1	pm-admin1
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]**.





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 – <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 – <ul style="list-style-type: none"> • 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 – <ul style="list-style-type: none"> • 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 –

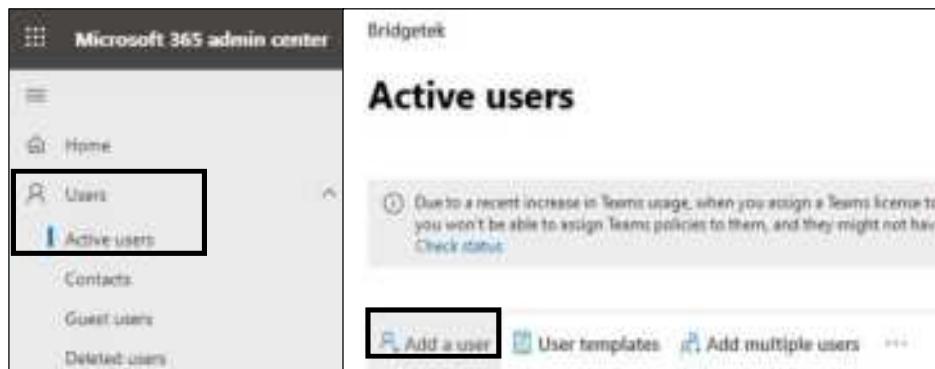
→ Login to Microsoft 365 Admin Center Console

- 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**].

Add a user

Assign product licenses

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

Select location *

Singapore

Licenses (0) *

Assign user a product license

Microsoft 365 Business Standard
24 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.

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

Add a user

Optional settings

You can choose what role you'd like to assign for this user and add additional profile information.

Role (User: no administrative access)

Admin roles give users permission to view data and complete basic management tasks. Give users only the access they need by assigning the least permission role.

[Learn more about admin roles](#)

User (User: no administrative access)

Admin center access

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

Exchange admin

Cloud admin

Global reader

Helpdesk admin

General support admin

Back Next Cancel

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

Add a user

Review and finish

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

Display and username
User1
user1@bridgeok.com
Title:

Password
Save Custom password
Send To: administrator@bridgeok.com
E-Mail:

Product licenses
Location: Singapore
Licenses: Microsoft 365 Business Standard
Apps: Power Virtual Agents for Office 365, Common Data Service for Teams, Project for Office (Plan E3), 25 more
Total:

Role Defaults
User (no admin or owner access)

Back **Finish adding** **Cancel**

Add a user

User1 added to active users

User1 will now appear in your list of active users.

User details
Display name: User1
Username: user1@bridgeok.com
Password: ***** Show
Sending to: administrator@bridgeok.com

Licenses bought
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 details, 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	Licenses
Administrator Bridgetek	Administrator@bridgetek.com	Microsoft 365 Business Standard
Room 1	Room 1@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”.

Exchange admin center

Recipients **Groups**

New Microsoft 365 group

DISPLAY NAME	TYPE	STATUS
All Company	Mail-enabled security group Dynamic distribution list	Active

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

new distribution list

*Display name:
jdm-user-group-testgroup1

*Title:
jdm-user-group-testgroup1

*Email address:
jdm-user-group-testgroup1@outlook.com

Notes:

*Owners:
+ -
Administrator

Members:
 Add group members as members
+ -

Choose whether user approval is required to join the group.

Open Anyone can join this group without being approved by the group owners.

Owner Members can be added only to the owner's members. All requests to join will be reviewed automatically.

Owner approve. All requests are approved or rejected by the group owners.

Save **Cancel**

- The newly added distribution list is displayed.

Exchange admin center

Mailboxes groups resource contacts shared migration

Try the new Exchange

Use the latest version of the Outlook.com available on the Groups page of the new Exchange admin center.

Groups

New Microsoft 365 group

Display name	Group type	+	Mail	More options
jdm-user-group-testgroup1	Distribution list	-	jdm-user-group-testgroup1@outlook.com	jdm-user-group-testgroup1

UPGRADE

Microsoft 365 (E3)



→ Create Desk / Resource Account

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with options like Home, User, Groups, Roles, Resources, and Rooms & equipment. The 'Rooms & equipment' option is selected and highlighted with a red box. The main area is titled 'Rooms & equipment' and contains a table with columns for Name, Email, and Type. At the top right of this area, there's a 'Add resource' button, which is also highlighted with a red box.

- 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 @ bridgetek.com

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

Domains

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.



Name	Email	Type
Desk1	Desk1@bridgetek.com	Room

→ 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: Domain:

Password settings:

Auto-generate password
 Let me 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].

Add a user

Assign product licenses

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

Select location:

Licenses (1):

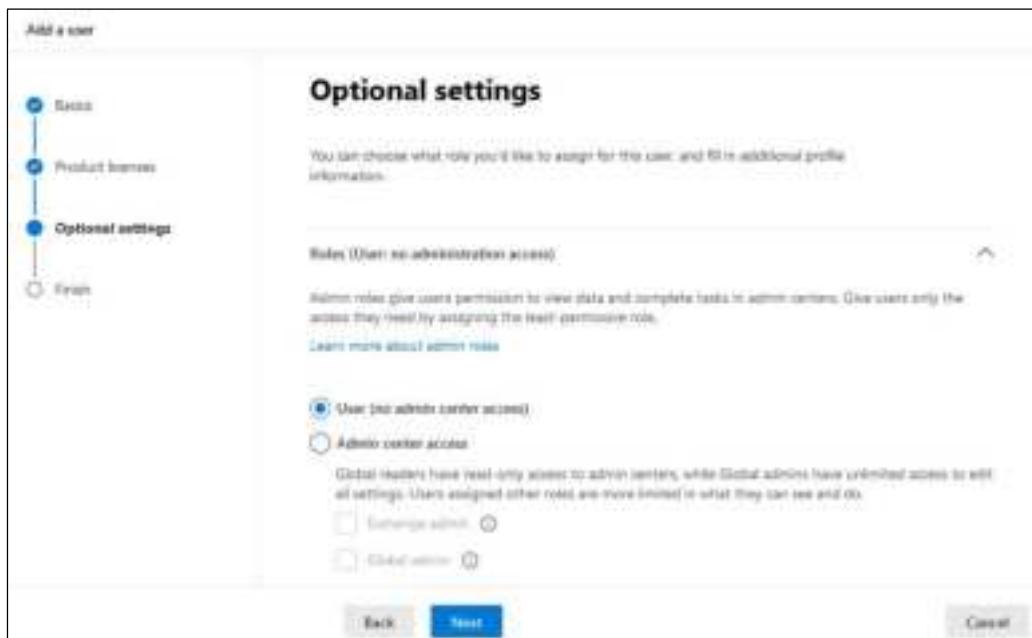
Assign user a product license
 Microsoft 365 Business Standard
11 of 25 licenses available

Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

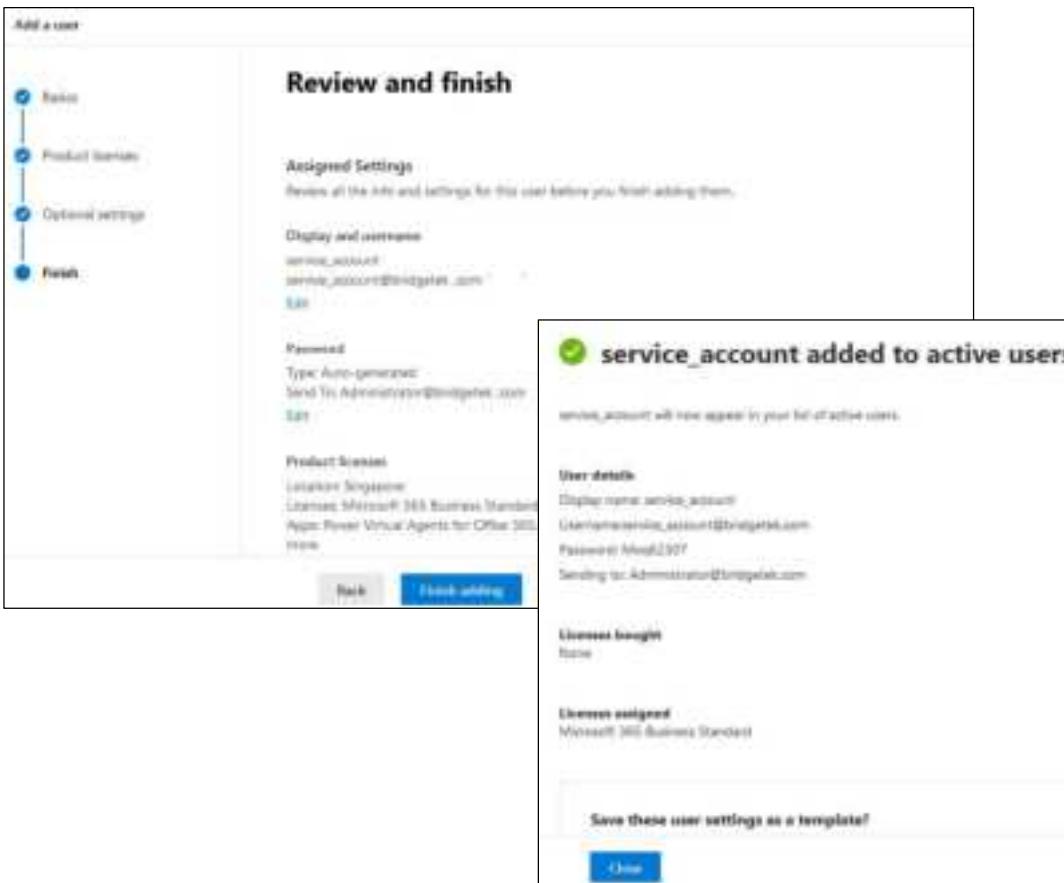
Apps (2):

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.

The screenshot shows the 'Active users' page in the Microsoft 365 Admin Center. At the top, there are buttons for 'Add a user', 'User templates', and 'Add multiple users'. Below these are filters and search fields. The main table lists users with columns for 'Display name', 'Username', and 'License'. One user, 'Administrator@bridgeit.com', has a Microsoft 365 Business Standard license. Another user, 'Room', is unlicensed. The third user, 'service_account', is highlighted with a black border. The 'service_account' row shows the email address 'service_account@bridgeit.com' and a Microsoft 365 Business Standard license.

Display name	Username	License
Administrator Bridgeit	Administrator@bridgeit.com	Microsoft 365 Business Standard
Room	Room@bridgeit.com	Unlicensed
service_account	service_account@bridgeit.com	Microsoft 365 Business Standard

→ 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**”.

The screenshot shows the 'Exchange admin center' with the 'admin roles' tab selected. On the left, there's a sidebar with various management categories like compliance management, organization, protection, mail flow, public folders, unified messaging, servers, and hybrid. The 'permissions' category is also visible. The main area displays a list of roles with a 'Discovery Management' role selected. This role includes several sub-options such as Help Desk, Hygiene Management, Organization Management, Public Folder Management, Recipient Management, Records Management, Security Administrator, Security Reader, Server Management, UIM Management, and View-Only Organization Management.

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

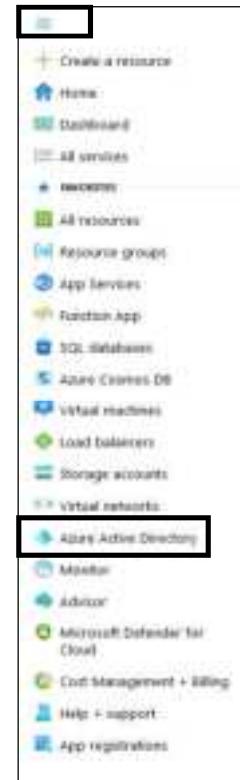


- Similarly, click “+” under “**Members**” and add the service account and click **[OK]**. Service account will be added and displayed. Click **[Save]**.



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

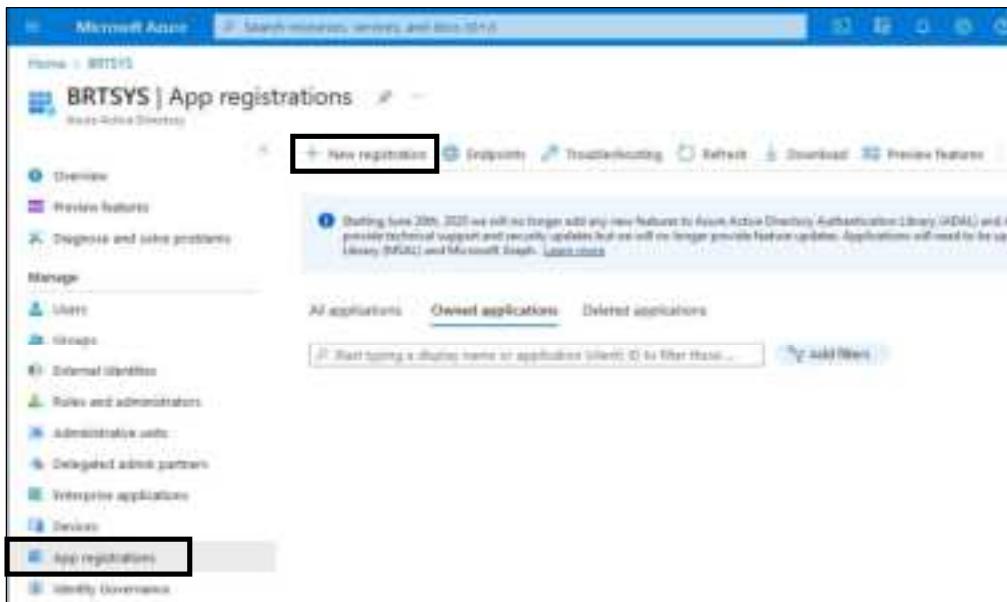
- Access Azure Portal using the administrator account - <https://portal.azure.com>
- Go to **Azure Active Directory** from the left navigation menu.
 - Register Applications
 - Setup Authentication (Redirect URI)
 - Setup Client Secret
 - Setup API Permissions



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**].

Name: PDM Client

Supported account types:

What can this application access via API?

Accounts in the organizational directory only (B2B2C 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 Terms.

Register

- The PDM Client application is successfully created.

PDM Client

Display name: PDM Client

Application ID: 19021003-0f4d-4f0d-9f47-10220200

Tenant ID: 19121003-0f4d-4f0d-9f47-10220200

Supported account types: Accounts in this organization directly only

Get Started Documentation



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]**.

Description	PDM Client Secret
Expires	730 days (24 months)
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

- 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.

The screenshot shows the 'Certificates & secrets' section of the Azure portal. A client secret named 'PDM Client' is listed. The secret value is '1234567890'. The secret is set to expire on 9/1/2023. The secret is currently valid.

5.2.2.1.4 Setup API Permissions

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

The screenshot shows the 'API permissions' section of the Azure portal. A new permission is being added for 'Office 365 Exchange Online'. The permission is named 'Read all items in my inbox'.

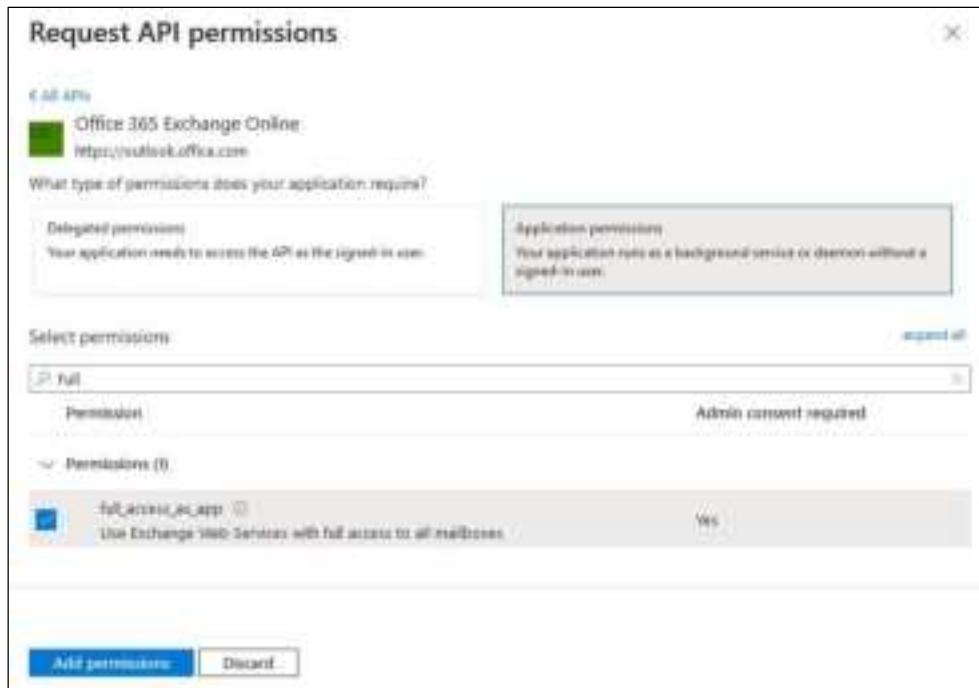
- Go to the **APIs my organization uses** tab, type **Office 365** in the search bar; Click and select **Office 365 Exchange Online** from the search result.

The screenshot shows the 'Request API permissions' dialog box. The search bar contains 'OFFICE 365'. The results list 'Office 365 Exchange Online' under the 'My APIs' tab.

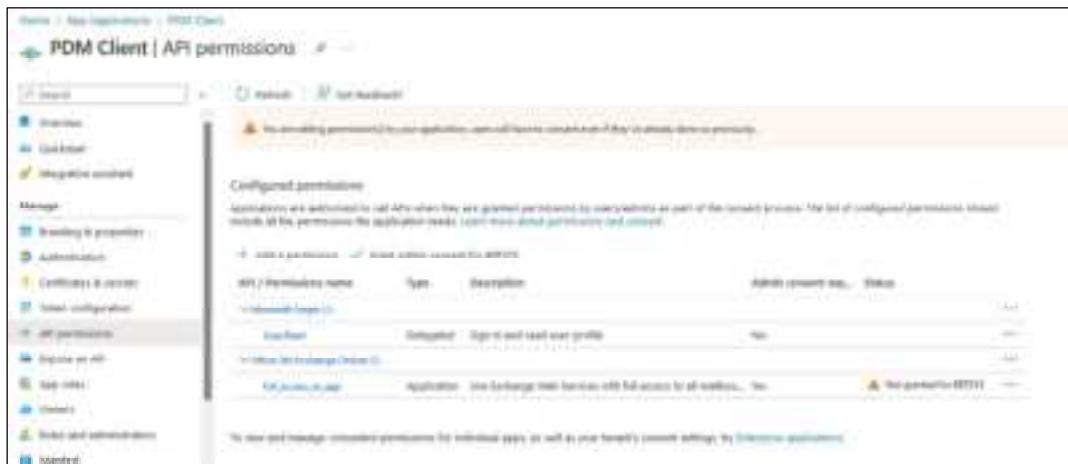
Name	Application (client) ID
Office 365 Enterprise Insights	fbd02341-e7aa-456d-925d-4abca9ff0f8e
Office 365 Exchange Online	00000003-0000-0000-0000-000000000000
Office 365 Information Protection	2f3802c9-9d79-4ad5-a625-0de55b07d135
Office 365 Management APIs	c5300580-fb23-4401-95e0-b4b7a6ef2fc2
Office 365 Search Service	66w88757-25a1-4c71-893c-3e3bed4d8869
Office 365 SharePoint Online	00000003-0000-0000-0000-000000000000



- 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.



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.

API Permissions name	Type	Description	Admin consent req.	Status
Microsoft Graph (1)	Delegated	Sign-in and read user profile	No	Granted to BRTSYS
Office 365 Exchange Online (1)	Delegated	Read settings, full mailbox with full access to all mailboxes... No	No	Granted to BRTSYS
Office 365 Exchange Online (2)	Application	Read settings, full mailbox with full access to all mailboxes... No	No	Granted to BRTSYS

5.2.2.1.5 Setup Delegate Permissions

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

API Permissions name	Type	Description	Admin consent req.	Status
Microsoft Graph (1)	Delegated	Sign-in and read user profile	No	Granted to BRTSYS
Office 365 Exchange Online (1)	Delegated	Read settings, full mailbox with full access to all mailboxes... No	No	Granted to BRTSYS
Office 365 Exchange Online (2)	Application	Read settings, full mailbox with full access to all mailboxes... No	No	Granted to BRTSYS

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

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Extra (D, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner), and more through a single endpoint.

Azure Rights Management Services

Allow authorized users to read and write protected content.

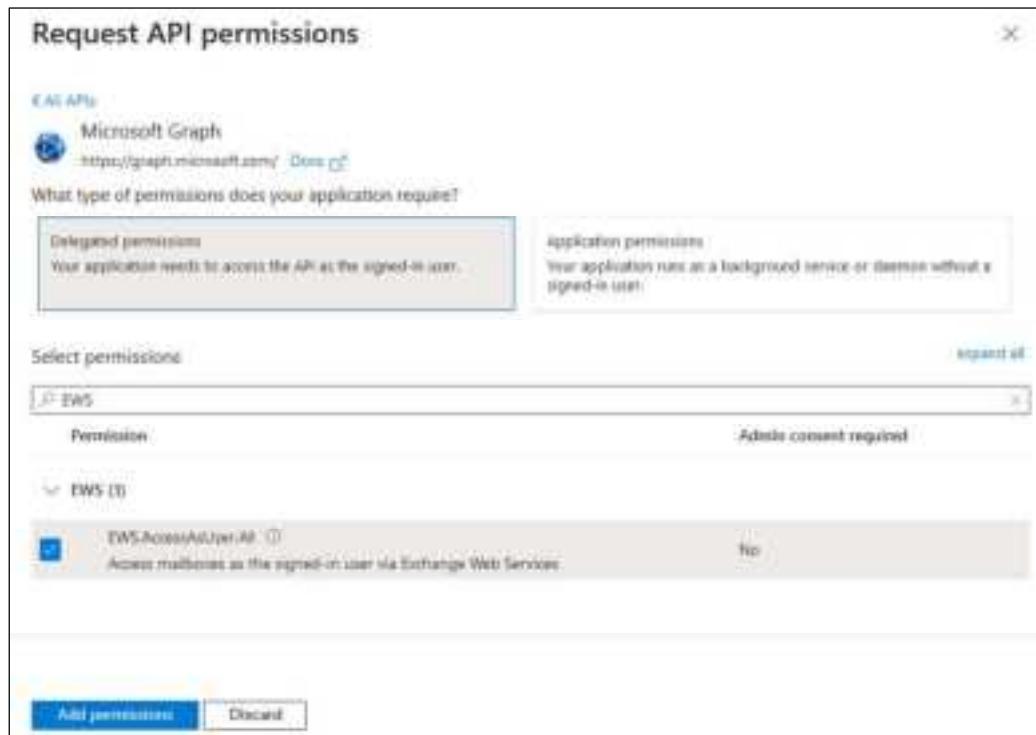
Azure Service Management

Programmatic access to much of the functionality available through the Azure portal.

Dynamics CRM

Access the capabilities of CRM Business software and ERP systems.

- 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.

API Permissions Name	Type	Description	Admin Consent Status
User.read	Delegated	Allow read-only access to the signed-in user via Exchange Web Services	Granted for BRTSYS
User.read.all	Delegated	Allow read/write access to all users using OAuth 2.0	Granted for BRTSYS
User.read.writeValue	Delegated	Allow to set email user profile	Granted for BRTSYS
User.read.all.writeValue	Application	Allow Exchange Web Services to read/write to all profiles	Granted for BRTSYS

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.

API Permissions Name	Type	Description	Admin Consent Status
User.read	Delegated	Allow read-only access to the signed-in user via Exchange Web Services	Granted to BRTSYS
User.read.all	Delegated	Allow read/write access to all users using OAuth 2.0	Granted to BRTSYS
User.read.writeValue	Delegated	Allow to set email user profile	Granted to BRTSYS
User.read.all.writeValue	Application	Allow Exchange Web Services to read/write to all profiles	Granted to BRTSYS



Note: More platforms and URLs 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]**.

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

Supported account types:
Who can use this application or access its API:
 Accounts in this organizational directory only (Microsoft Entra ID) (single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant) (multi-tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - multi-tenant and personal Microsoft accounts) (e.g., Skype, Bing)
 Personal Microsoft accounts (me)

[Help me choose...](#)

Redirect URI (optional):
With whom the authentication requests 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.

[Register an app you're writing or have integrated with your app and other app from another organization by adding from a enterprise application...](#)

By proceeding, you agree to the Microsoft Platform Terms of Use.

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.

- 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**.

The screenshot shows the 'Certificates & secrets' page with the 'Client secrets' tab selected. A new client secret named 'PDM Add-In Client Secret' is listed with the following details:

- Description:** PDM Add-In Client Secret
- Expires:** 130 days (24 months)
- Value:** (Visible only to the user who created it)
- Secret ID:** (Visible only to the user who created it)

A note at the bottom states: 'No client secrets have been created for this application.'

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

The dialog box has the following fields:

- Description:** PDM Add-In Client Secret
- Expires:** 130 days (24 months)
- Add** (highlighted)
- Cancel**

- 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.

The screenshot shows the 'Certificates & secrets' page with the 'Client secrets' tab selected. The newly created client secret is listed with the following details:

- Description:** PDM Add-In Client Secret
- Expires:** 130 days (24 months)
- Value:** (Visible only to the user who created it)
- Secret ID:** (Visible only to the user who created it)

A note at the bottom states: 'Client secret values cannot be viewed except for immediate after creation. Be sure to copy the secret value copied before leaving the page.'



5.2.2.3 Mobile Client

5.2.2.3.1 App Registration

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Home > BRTSYS' and 'Azure Active Directory'. Below this, the 'App registrations' section is displayed. On the left, there's a sidebar with options like 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage' (with sub-options like 'Users', 'Groups', 'External identities', etc.), and 'App registrations' (which is highlighted with a red box). At the top right, there are buttons for 'Inquiries', 'Troubleshooting', 'Feedback', 'Download', and 'Preview features'. A central message states: 'Starting April 2020, we will no longer add new features to Azure Active Directory Authentication Library (ADAL) and no longer provide technical support and security updates for it. We will no longer provide feedback available. Applications will need to use ADALv2 and Microsoft Identity Platform instead.' Below this message, there are tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications'. A search bar at the bottom says 'Start typing a display name or application ID to filter them...' and a 'Search' button.

- 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 screenshot shows the 'Register an application' form. At the top, it says 'Home > App registrations > Register an application'. The 'Name' field is filled with 'PDM Mobile Client'. The 'Supported account types' section contains the following options:

- 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, MSN, etc.)
- Personal Microsoft accounts only

 Below this is a 'Help me choose...' link. The 'Redirect URI (optional)' section has a note: 'We'll return the authentication responses to this URL 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.' It shows a dropdown set to 'Select a platform' and a text input with 'e.g. https://example.com/auth'. At the bottom, there's a note: 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#)'. A disclaimer: 'By proceeding, you agree to the Microsoft Platform Terms of Use.' and a 'Register' button.

- The PDM Mobile Client application is successfully created.

The screenshot shows the 'App registrations' section of the Azure portal. A specific application named 'PDM Mobile Client' is selected. In the 'Certificates & secrets' section, two entries are listed: 'Client ID' (22a8fbcf-00ff-441d-94a2-0aef01010101) and 'Object ID' (a000c000-0000-4000-9000-000000000000). The 'Secret' field is shown as 'Not set'.

5.2.2.3.2 Setup Authentication (Redirect URI)

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

The screenshot shows the 'Authentication' page for the 'PDM Mobile Client'. Under 'Platform configurations', the 'Web' option is selected. To the right, a 'Configure platforms' sidebar is open, showing the 'Web' configuration section with options for 'Single sign-on' and 'Mobile and desktop applications'.

- 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 screenshot shows the 'Configure Web' dialog. Under 'Redirect URIs', the value 'https://api.pdm.local/api/user/oidc-login' is entered. Below it, under 'Front-channel logout URL', there is a placeholder 'e.g. https://example.com/logout'. At the bottom, the 'ID tokens could be required for implicit flows' checkbox is checked.

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

The screenshot shows the 'Web' configuration section. It includes fields for 'Redirect URI' (with a placeholder 'https://api.pdm.local/api/user/v2/oidc-login-callback') and 'Front-channel logout URI' (with a placeholder 'https://localhost/logout'). Below these fields is a note about hybrid grants and hybrid flows. At the bottom right of the configuration area, there is a blue rectangular button labeled 'Add URI' with a '+' icon, which is highlighted with a red box.

- 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

The screenshot shows the 'Web' configuration section after adding two new redirect URIs. The 'Redirect URI' field now contains two entries: 'https://api.pdm.local/api/user/v2/oidc-login-callback' and 'https://localhost/logout'. The 'Front-channel logout URI' field also contains 'https://localhost/logout'. The 'Add URI' button is no longer highlighted.

- 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**.

Description	Expires	Value	Secret ID
PDM Mobile Client Secret	Never	XXXXXXXXXXXXXX	XXXXXXXXXXXXXX

- 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.

Description	Expires	Value	Secret ID
PDM Mobile Client Secret	Never	XXXXXXXXXXXXXX	XXXXXXXXXXXXXX



5.2.2.4 PDM Management Console (WMC Client)

5.2.2.4.1 App Registration

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

The screenshot shows the Microsoft Azure portal interface under the 'Azure Active Directory' section. The left sidebar has 'App registrations' selected. The main area shows a message about deprecating legacy authentication libraries, followed by tabs for 'All applications', 'Created applications' (which is selected), and 'Deleted applications'. Below is a search bar and a 'New application' button.

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

The screenshot shows the 'Register an application' form. The 'Name' field is set to 'PDM WMC Client'. Under 'Supported account types', the option 'Accounts in this organizational directory only (BRTSYS-only - Single Tenant)' is selected. The 'Redirect URI (optional)' field contains 'http://www.brtsys.com/test'. At the bottom, there is a note about accepting the Microsoft Platform Policy, and a 'Register' button.

- The PDM WMC Client application is successfully created.

The screenshot shows the 'PDM WMC Client' application interface. On the left, there's a navigation sidebar with options like 'Overview', 'Dashboard', 'Integration assistant', 'Manage', 'Adding an application', 'Authentication', 'Integrate API services', 'Token configuration', 'API permissions', and 'Logout URL'. The main area has a heading 'Get started' and a sub-section 'Configure platforms'. A callout box highlights the 'Properties' section, which displays the following details:

- Display name:** PDM WMC Client
- Redirect URI:** https://api.pdm.local/api/user/oidc-login
- Object ID:** f1e3a88e-825a-48ff-91011f8a6a
- Directory Identifier ID:** b2e9f9e0-2080-446f-970d-2aef770101
- Associated external login:** https://organizations.local

5.2.2.4.2 Setup Authentication (Redirect URI)

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

The screenshot shows the 'Authentication' page. The left sidebar includes 'Overview', 'Dashboard', 'Integration assistant', 'Manage', 'Integrate API services', 'Token configuration', 'API permissions', 'Logout URL', 'Integrate', 'Logout', 'Integrate API services', 'Integrate', 'Logout', 'Integrate', 'Logout', and 'New support request'. The main area has a heading 'Platform configurations' and a sub-section 'Supported account types'. A callout box highlights the 'Add a platform' button. To the right, there's a 'Configure platforms' sidebar with sections for 'Web applications' (selected), 'Mobile and mobile web applications' (disabled), 'Mobile and mobile web applications' (disabled), and 'Mobile and desktop applications' (disabled).

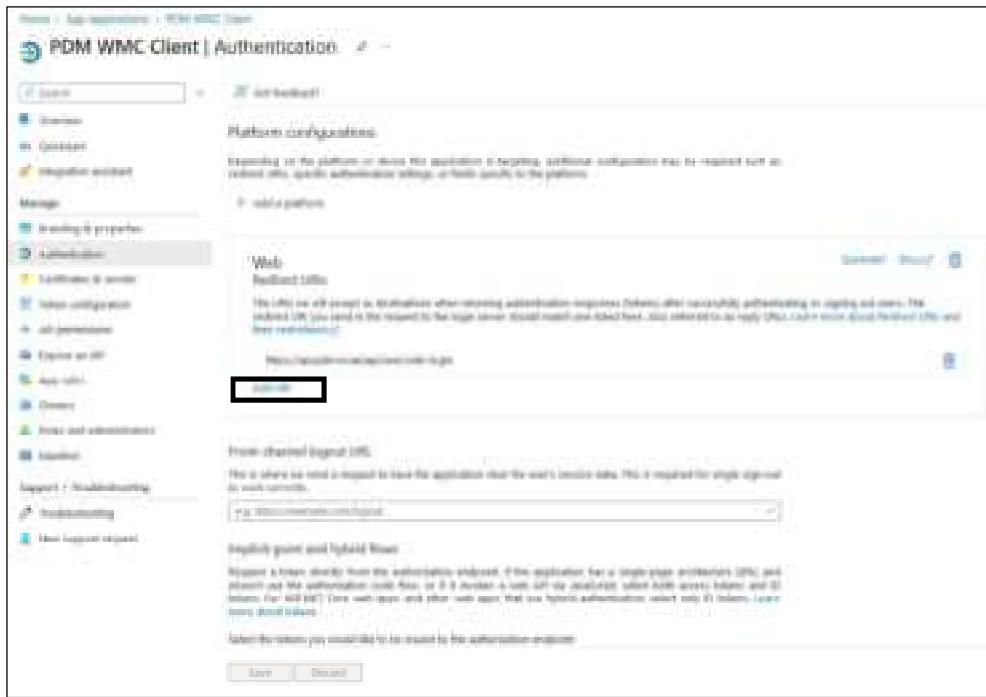
- In the configure Web UI –

- 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 screenshot shows the 'Configure Web' dialog. It has sections for 'Front-channel logout URL' (set to https://api.pdm.local/api/user/logout) and 'Implicit grant and hybrid flows'. The 'Implicit grant and hybrid flows' section is expanded, showing the following options:

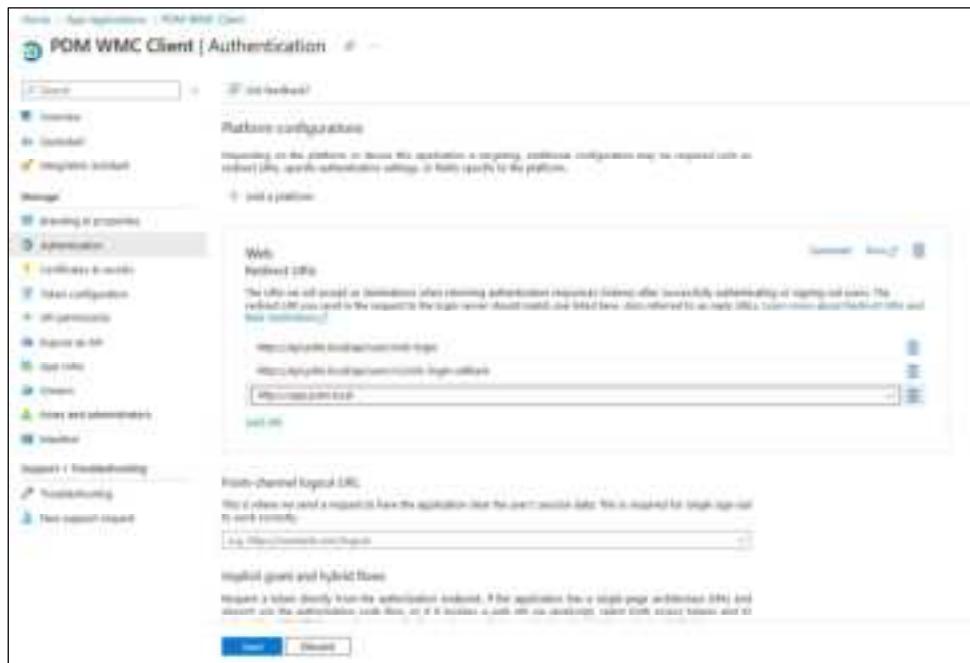
- Implicit grant and hybrid flows:** Requests a token directly from the authorization endpoint. If the application has a single-page application (SPA), and doesn't use the auth code flow, or if it involves a web app, use JavaScript, select both access tokens and ID tokens. For hybrid SPA and web, and offline web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.
- Code access:** The token you intend to be issued by the authorization endpoint.
- As code-accessed client for implicit flows:** (checked)
- As code-accessed client for hybrid flows:**

- 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**.

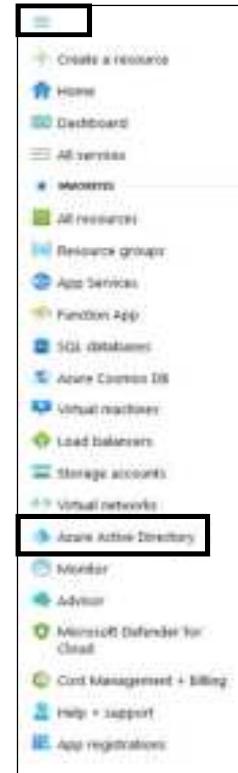
- In the **Add a client secret UI**, enter the *Description*; choose an *expiration period* and click **[Add]**.

- 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

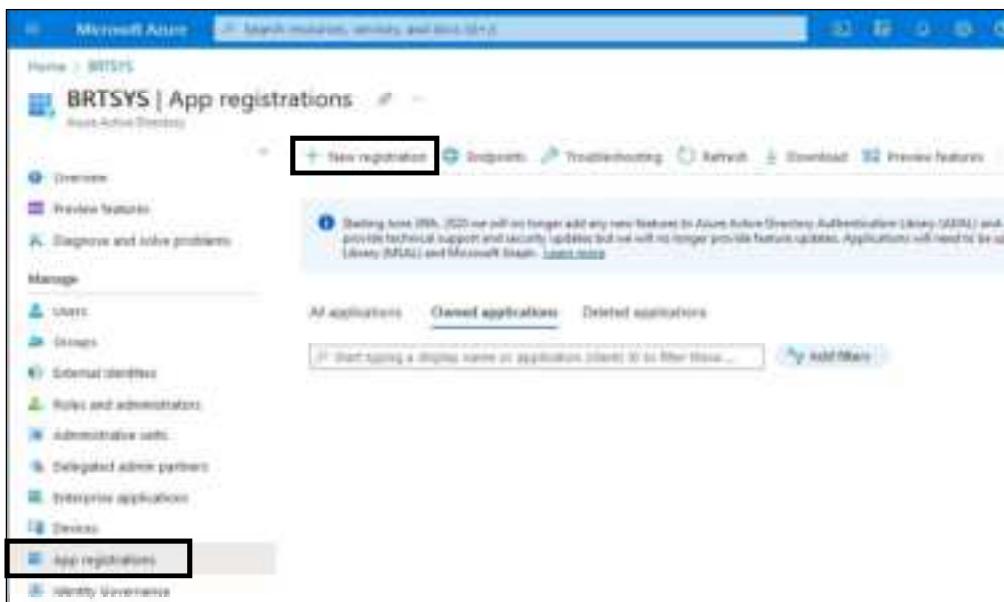
- Access Azure Portal using the administrator account – <https://portal.azure.com>.
- Go to **Azure Active Directory** from the left navigation menu.



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**].

Name: PDM Client ROPC
Supported account type:
 Accounts in this organizational directory only (Single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant) (Multi-tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant) - Administrators and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
Register

- The PDM Client ROPC application is successfully created.

Identifier URI	Secret
https://pdmclientropc.onmicrosoft.com	XXXXXXXXXXXXXX



5.2.3.1.2 Setup Authentication

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

Platform configurations:
Depending on the platform or model this application is targeting, additional configuration may be required such as custom OAuth-specific authentication settings, or facets specific to the platform.

Supported account types:
Who can use this application to access the API?
 Accounts in this organizational directory only (BRTSYS only - Single tenant)
 Accounts in any of organizational directories (Multi-tenant - Multi-tenant)

Advanced settings:

Allow public client flows Edit

Enable the following service and identity flows:

- App client credential password (Resource Owner Password Credential Flow) Edit
- User Refresh Token (User Refresh Token Flow) Edit
- ID token (JWT-based) (Implicit Grant Flow) Edit

App instance property lock Edit

Configure the application instance modification lock Edit

→ Click **[Save]**.

5.2.3.1.3 Setup API Permissions

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

API / Permission name	Type	Description	Update consent req. (Status)
User Read (User Read, User Read Data, User Profile)	User Read	User Read, User Read Data, User Profile	No

To view and manage consented permissions for this application, as well as your tenant's consent settings, try [Enterprise applications](#).

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

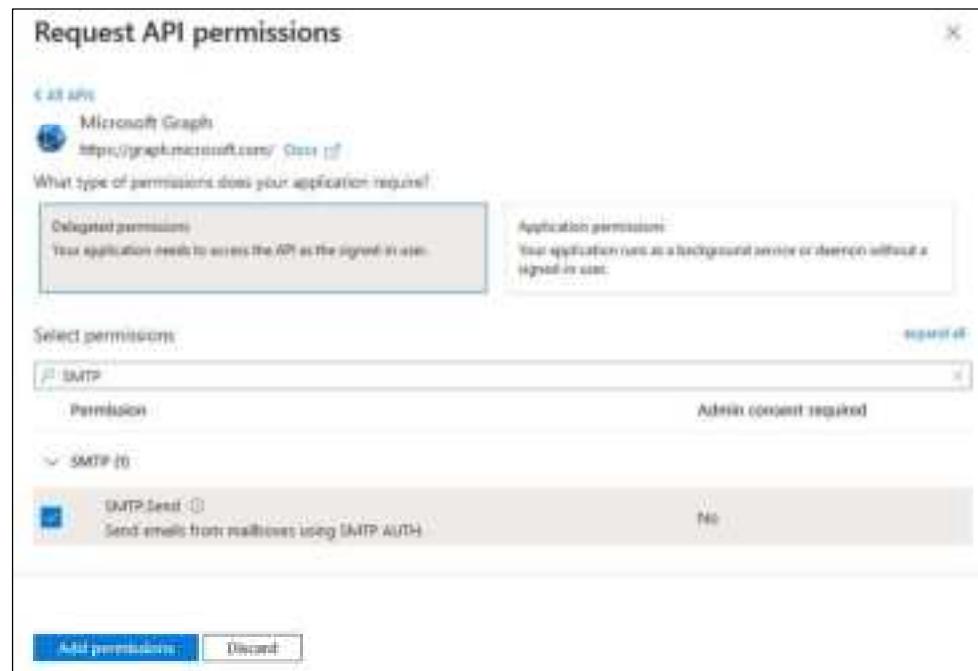
The screenshot shows the 'Request API permissions' interface. At the top, there's a navigation bar with tabs: 'Select an API', 'Microsoft APIs' (which is underlined), 'APIs my organization uses', and 'My APIs'. Below this, a section titled 'Commonly used Microsoft APIs' lists several services:

- Microsoft Graph**: Described as taking advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. It integrates Microsoft Data (i.e. Excel, Power, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more) through a single endpoint.
- Azure Rights Management Service**: Allows validated users to read and write protected content.
- Azure Service Management**: Programmatic access to much of the functionality available through the Azure portal.
- Dynamics CRM**: Access the capabilities of CRM business software and ERP systems.
- Intune**: Programmatic access to Intune data.
- Office 365 Management APIs**: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Intune (i.e. activity logs).
- OneNote**: Create and manage notes, lists, pictures, files, and more in OneNote notebooks.

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

The screenshot shows the 'Request API permissions' interface for the Microsoft Graph API. It displays two sections: 'Delegated permissions' and 'Application permissions'. Under 'Delegated permissions', the 'EWS' permission is selected. The 'EWS (5)' permission is also listed. Under 'Application permissions', there is one entry: 'EWS.AccessAsUser.All' (1) with the note 'Access mailboxes as the signed-in user via Exchange Web Services'. At the bottom, there are 'Add permissions' and 'Discard' buttons.

- 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.

API Permissions Name	Type	Description	Admin consent req'd
Microsoft Graph API	Delegated	Access Mailbox as the signed-in user or delegate user	No
SMTP.Send	Delegated	Send emails from millions using SMTP AUTH	No
User.Read	Delegated	Sign in and read user profile	No

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.

The screenshot shows the 'API permissions' section of the Microsoft Azure portal. The left sidebar lists several application permissions, with 'API permissions' selected. The main area displays a table of configured permissions:

API / Permissions name	Type	Description	Admin consent req.	Status
API User Read	Delegated	Access read-only to the signed-in user via Exchange Online	No	Granted to BRTSYS#077
API User ReadWrite	Delegated	Read and write to mailbox using EWS API (full rights)	No	Granted to BRTSYS#077
User Read	Delegated	Read by and read user profile	No	Granted to BRTSYS#077

Below the table, a note says: 'To view and manage consented permissions for individual apps, or with all your bound consent settings, try [View other app permissions](#)'.

6. Appendix

6.1 Exchange Server setup using Exchange Management Shell – Quick Reference

→ Open Exchange Management PowerShell as an Administrator	<p>a. From the exchange server, click Start → Microsoft Exchange Server → Exchange Management Shell. Right-click Exchange Management Shell and select "Run as administrator".</p> <p>b. The <i>Exchange Management Shell</i> is opened.</p> 
→ Create User Account	<p>c. Create user account using the following command –</p> <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	<p>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.</p> <p>d. Create a new user distribution group named "<i>pdm-user-group-<groupname></i>" using the following command –</p> <pre>New-DistributionGroup -Name "pdm-user-group-bridgetek1"</pre> <p>Note: A distribution group name should begin with prefix <i>pdm-user-group</i> and be followed by the group name.</p>
	<p>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 –</p> <pre>Add-DistributionGroupMember -Identity "pdm-user-group-bridgetek1" -Member user1@bridgetek.com</pre> <p>f. Use the following command to display a list of users who have been added to a particular distribution group –</p> <pre>Get-DistributionGroupMember -Identity "pdm-user-group-bridgetek1"</pre>
→ Create Desk / Resource Account	<p>g. Using the following command, create a resource account –</p> <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.



	<p>h. Create a new desk distribution group named "pdm-desk-group-<groupname>" using the following command -</p> <pre>New-DistributionGroup -Name "pdm-desk-group-bridgeTek1" -RoomList</pre> <p>Note: A distribution group name should begin with prefix <i>pdm-desk-group</i> and be followed by the group name.</p>
	<p>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 -</p> <pre>Add-DistributionGroupMember -Identity "pdm-desk-group-bridgeTek1" -Member desk1@bridgeTek.com</pre> <p>j. Use the following command to display a list of desks that have been added to a particular distribution group -</p> <pre>Get-DistributionGroupMember -Identity "pdm-desk-group-bridgeTek1"</pre>
→ Create Impersonation User / Service Account	<p>k. Create Service Account using the following command -</p> <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	<p>l. Create Admin Role Group and Grant Service Account Impersonation Rights using the following command -</p> <pre>New-RoleGroup -Name "Application Impersonation Role" -Roles "ApplicationImpersonation" -Members service-account@bridgeTek.com</pre> <p>m. Using the following command, view the application impersonation data -</p> <pre>Get-ManagementRoleAssignment -Role "ApplicationImpersonation" -GetEffectiveUsers</pre>
→ Discovery Management	<p>n. Using the following command, add the service account into Discovery Management Role -</p> <pre>Add-RoleGroupMember -Identity "Discovery Management" -Member service-account@bridgeTek.com</pre> <p>o. View the list of members in the Discovery Management Role, using the following command -</p> <pre>Get-RoleGroupMember -Identity "Discovery Management"</pre>



6.2 Microsoft 365 setup using Windows PowerShell – Quick Reference

<p>→ Open Windows PowerShell as an Administrator</p>	<ul style="list-style-type: none"> 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> <ul style="list-style-type: none"> c. Using the following command, import the Exchange Online Management Module – <pre>\$ Import-Module ExchangeOnlineManagement</pre> <ul style="list-style-type: none"> d. Using the following command connect to the Exchange Online Management Module. <pre>Connect-ExchangeOnline -UserPrincipalName Administrator@bridgetek.com</pre> <p>Now the Microsoft 365 can be managed via PowerShell.</p>
<p>→ Create User Account</p>	<ul style="list-style-type: none"> 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>
<p>→ Create Distribution Group for Users</p>	<p>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.</p> <ul style="list-style-type: none"> 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> <p>Note: A distribution group name should begin with prefix <i>pdm-user-group</i> and be followed by the group name.</p>
	<ul style="list-style-type: none"> f. 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> <ul style="list-style-type: none"> 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>
<p>→ Create Desk / Resource Account</p>	<ul style="list-style-type: none"> h. Using the following command, create a resource account – <pre>New-Mailbox -Name "Desk1" -DisplayName "Desk1" -Room</pre>



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