

# PANL

Room Manager 3.1.1

## Part 2 - Installation and Configuration



Document Version: 2.0

Issue Date: 04-07-2024

# PANL

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

<b>1. About This Guide .....</b>	<b>3</b>
<b>2. Intended Audience .....</b>	<b>3</b>
<b>3. Document References .....</b>	<b>3</b>
<b>4. PRM Server Installation &amp; Configuration .....</b>	<b>4</b>
4.1 Hardware / Software Requirements .....	4
4.2 Network Port Requirements.....	4
4.3 Installing PRM on Linux Distribution Server (Ubuntu OS, RHEL, CentOS, OpenSUSE) .	5
4.4 SSL Certificate Setup .....	10
<b>5. Mail/Calendar Server Setup &amp; Configuration.....</b>	<b>11</b>
5.1 Exchange Server 2019/2016/2013 Setup .....	11
5.1.1 Using Exchange Admin Centre Console .....	12
5.2 Microsoft 365 Setup.....	21
5.2.1 Using Microsoft 365 Admin Center Console .....	22
5.2.2 Modern Authentication using OAuth 2.0 – Open ID-Connect (OIDC) .....	33
5.2.2.1 PRM Client .....	33
5.2.2.1.1 App Registration .....	33
5.2.2.1.2 Setup Authentication (Redirect URI).....	35
5.2.2.1.3 Setup Client Secret .....	36
5.2.2.1.4 Setup API Permissions.....	37
5.2.3 Modern Authentication using OAuth 2.0 - ROPC .....	40
5.2.3.1 PRM Client .....	40
5.2.3.1.1 App Registration .....	40
5.2.3.1.2 Setup Authentication .....	42
5.2.3.1.3 Setup API Permissions.....	42
<b>6. Appendix .....</b>	<b>46</b>
6.1 Exchange Server setup using Exchange Management Shell – Quick Reference .....	46
6.2 Microsoft 365 setup using Windows PowerShell – Quick Reference.....	49
6.3 Glossary of Terms, Acronyms & Abbreviations .....	51
6.4 List of Figures .....	51
6.5 List of Tables .....	51
<b>Revision History .....</b>	<b>52</b>

## 1. About This Guide

This guide explains the Installation/Setup & Configuration of PRM Server, Mail Server and Calendar Server. **The screenshots used are for illustration purpose 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
<a href="#">BRTSYS AN 037 PRM User Guide - 1. Introduction</a>	Application Note (User Guide)	PDF
<a href="#">BRTSYS AN 039 PRM User Guide - 3. PRM Management Console</a>		
<a href="#">BRTSYS AN 040 PRM User Guide - 4. PRM Supervisor and PanLHub Supervisor Console</a>		
<a href="#">BRTSYS AN 041 PRM User Guide - 5. Outlook Add-In</a>		
<a href="#">BRTSYS AN 042 PRM User Guide - 6. PanL PD100 Touch Display</a>		

## 4. PRM Server Installation & Configuration

### 4.1 Hardware / Software Requirements

Hardware / Software	Specifications		
Server Hardware Requirements	Processor –i7 dual core Hard disk – 50GB RAM – 4GB RAM (minimum)		
Operating System	Linux based OS (Ubuntu 20.04 LTS/ RHEL 8.6/ OpenSUSE Leap 15.4/CentOS Linux 7) onwards		
Exchange Server	Microsoft Exchange 2013/2016/2019 & Microsoft 365		
Database Software	PostgreSQL		
Console Web Browser	Chrome v65+/Safari/Microsoft Edge		
Client Software	Outlook Add-In 2010/2013/2016/Outlook App Ensure that any of the above outlook versions are installed.		
Network Ports	Exchange Server	Port 443	Used for EWS connection
		Port 587 / Port 25	Used for SMTP
	PRM Server	Port 8081	Used for PRM Supervisor
		Port 443 / Port 4430	Used for API
		Port 3002	Used for Socket Notification
	Client (Outlook Add-In)	Port 5353	Used for mDNS
	PanLHub	Port 8081	Used for PanLHub Supervisor
		Port 4430	User for API
		Port 5353	Used for mDNS

**Table 1 – Hardware / Software Requirements**

### 4.2 Network Port Requirements

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

Source	Destination	Ports
PRM Server, Hub	Exchange server, O365, NTP server	443, 587, 25, 123
PRM Server	Hub	5353, 4430, 8081
Browser, Add-In, Hub	PRM Server	443, 4430, 5353, 8081
Hub	PRM Server	4430, 8081, 5353

**Table 2 – Network Port Requirements**

## 4.3 Installing PRM on Linux Distribution Server (Ubuntu OS, RHEL, CentOS, OpenSUSE)



**Note:** This section is applicable ONLY for SUPERADMIN User

- a. Copy both the PRM installation files to the location in which the server will be installed.



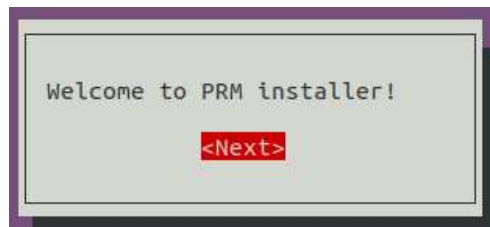
- b. Provide the executable permission to PRM Script file

```
$ sudo chmod +x PRM_Setup.sh
```

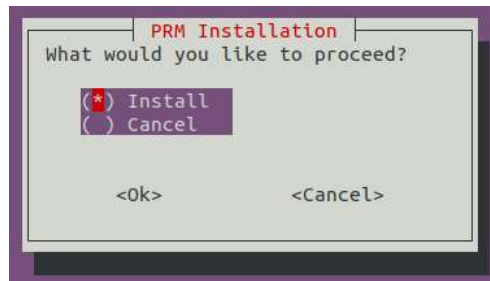
- c. Install PRM script.

```
$ sudo ./PRM_Setup.sh
```

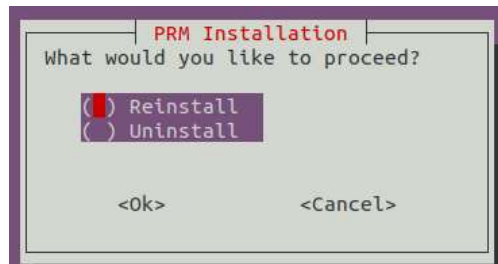
- d. PRM Installer welcome message will be displayed. Click **[Next]**.



- e. If the PRM package is installed for the first time, then the PRM Installation menu is displayed with following menu options – **[Install]** and **[Cancel]**.

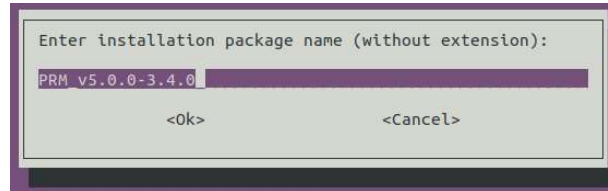


- f. If a previous version of PRM Software is installed before, then the PRM Installation menu is displayed with the following menu options – **[Reinstall]** and **[Uninstall]**.

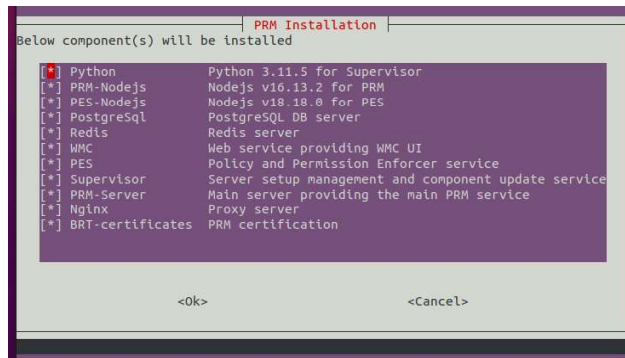


- g. Select **[Install]** to start a fresh installation; Select **[Reinstall]** to overwrite with the latest files (deleting all previous files); Select **[Uninstall]** to uninstall the PRM package.

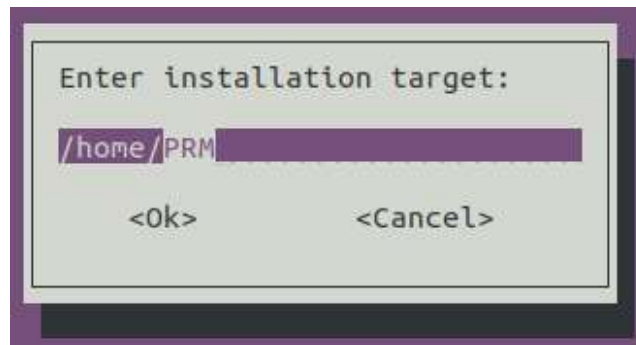
Upon selecting **[Install]**, click **[Ok]**. Installation package name is required. The package name will be auto filled-in by the system, click **[Ok]** to proceed.



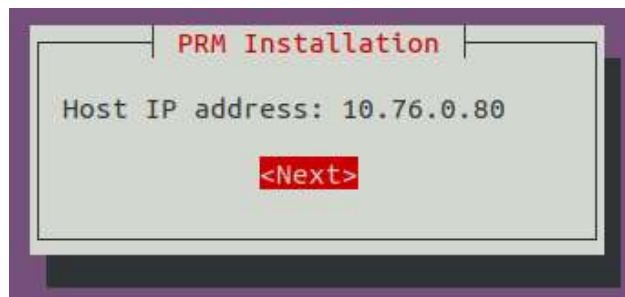
- h. A list of components that will be installed is displayed. Click **[Ok]**.



- i. User can provide a folder name, wherein the installation files are installed. For example, "PRM". Click **[Ok]** to proceed.

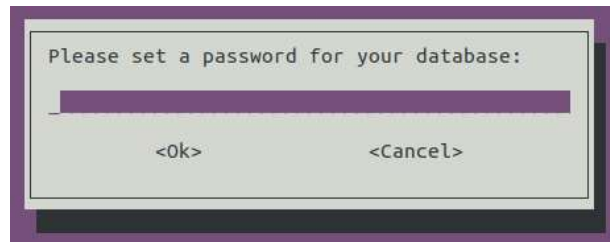


- j. The Host IP address is displayed. Click **[Next]** to proceed.

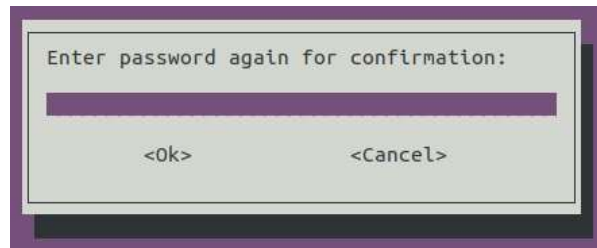




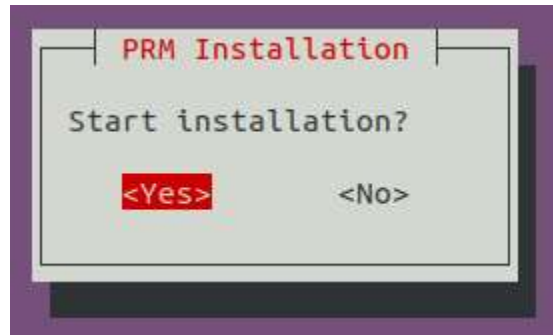
- k. Set a password and click **[Ok]**.



- l. Confirm the password and click **[Ok]**.



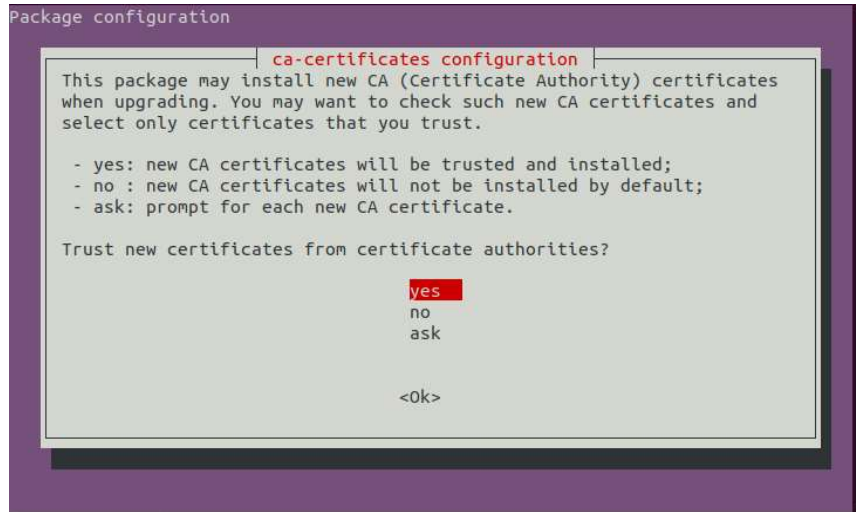
- m. Click **[Yes]** to start the installation.



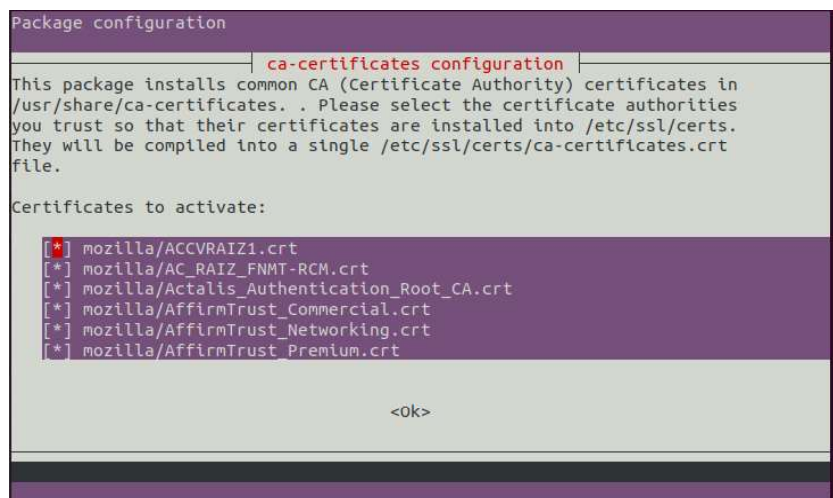
The installation will start and progress.

```
/tmp/PRM_v5.0.0-3.4.0/Services/Node/Common /home/administrator/PRM
Creating /opt/PRM/nodejs/v16.13.2 folder...
/home/administrator/PRM
Installing nodejs for PES
/tmp/PRM_v5.0.0-3.4.0/Services/Node/Common /home/administrator/PRM
Creating /opt/PRM/nodejs/v18.18.0 folder...
/home/administrator/PRM
Creating /home/PRM/PRM folder...
Creating /home/PRM/PRM/mrbs_logs folder...
Creating /home/PRM/PRM/Data folder...
Creating /home/PRM/PRM/Data/scratch folder...
Creating /home/PRM/PRM/Data/scratch/uploads folder...
Creating /home/PRM/PRM/Data/config folder...
Creating /home/PRM/PRM/Data/config/backup folder...
Creating /home/PRM/PRM/pid folder...
Creating /home/PRM/PRM/Hub folder...
Creating /home/PRM/PRM/Supervisor folder...
Creating /home/PRM/PRM/Web folder...
Creating /home/PRM/PRM/Pes folder...
Deploying main components...
Copying PRM
Configuring PRM 1/2
/home/PRM/PRM/Hub /home/administrator/PRM
```

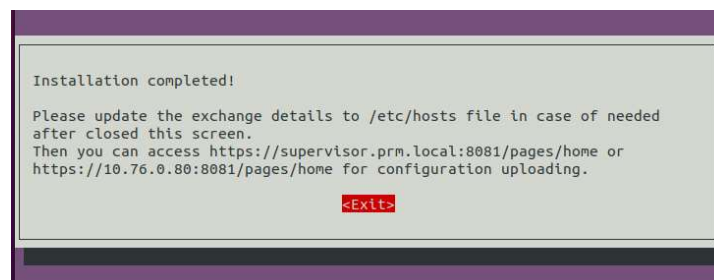
- n. A popup box may be triggered prompting installation of default Bridgetek's Certificate. Select **yes** to proceed or **no** to skip the default installation. Non-default certificates can be installed through the PanL Supervisor console. (Refer to PRM Supervisor section in [BRTSYS AN 029 PRM User Guide - 4. PRM and PanLHub Supervisor](#). If default Bridgetek's certificate is selected, please ensure that the SSL certificate is installed if using Client PC to run PRM https components (PRM Management Console/Add-In). Refer to [SSL Certificate Setup](#).



- o. If the default certificate is selected, another popup box will appear as below. Ensure that all listed certificates are selected and click **[Ok]**.



- p. Upon successful installation, an appropriate message indicating the same is displayed. Click **[Exit]**.





- q. Run the command given below to verify if **nginx service** is running-

```
$ sudo systemctl status nginx.service
```

```
administrator@administrator:/home/bridgetek$ sudo systemctl status nginx.service
● nginx.service - The NGINX HTTP and reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; disabled; vendor preset:
   Active: active (running) since Fri 2021-04-09 15:27:42 +08; 2min 15s ago
     Main PID: 16998 (nginx)
        Tasks: 2 (limit: 4657)
       Memory: 1.6M
      CGroup: /system.slice/nginx.service
              └─16998 nginx: master process /usr/sbin/nginx
                 └─16999 nginx: worker process

Apr 09 15:27:42 administrator systemd[1]: Starting The NGINX HTTP and reverse p
Apr 09 15:27:42 administrator nginx[16980]: nginx: the configuration file /etc/
Apr 09 15:27:42 administrator nginx[16980]: nginx: configuration file /etc/nginx
Apr 09 15:27:42 administrator systemd[1]: nginx.service: Failed to parse PID fr
Apr 09 15:27:42 administrator systemd[1]: Started The NGINX HTTP and reverse pr
lines 1-15/15 (END)
```

- r. To verify if the **PanL Node service** is running, use the command given below-  
(A PanLHub must be connected to the PRM Server for the Node service to be active)

```
$ sudo systemctl status panlnode.service
```

```
administrator@administrator:/home/bridgetek$ sudo systemctl status panlnode.serv
ice
● panlnode.service - PanL Node Service
   Loaded: loaded (/etc/systemd/system/panlnode.service; enabled; vendor pres
   Active: active (running) since Fri 2021-04-09 15:38:08 +08; 8s ago
     Main PID: 17203 (node)
        Tasks: 10 (limit: 4657)
       Memory: 146.9M
      CGroup: /system.slice/panlnode.service
              └─17203 /usr/local/bin/node ./src/index.js -- server=PRM config=.
Apr 09 15:38:14 administrator node[17203]: no sentinel key with the vendor code
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.894 - info: Couls
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.895 - info: ----
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.895 - info: Lice
Apr 09 15:38:14 administrator node[17203]: hasp_get_sessioninfo failed
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.897 - silly: Set
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.899 - verbose: De
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.911 - silly: sla
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.918 - silly: Sta
Apr 09 15:38:14 administrator node[17203]: 2021-04-09 15:38:14.918 - info: Time
lines 1-19/19 (END)
```

- s. Run the below command and verify PanL Supervisor service is running:

```
$ sudo systemctl status panlsupervisor.service
```

```
administrator@administrator:/home/bridgetek$ sudo systemctl status panlsupervis
r.service
● panlsupervisor.service - Panl Supervisor Service
   Loaded: loaded (/etc/systemd/system/panlsupervisor.service; enabled; vendo
   Active: active (running) since Fri 2021-04-09 15:27:59 +08; 13min ago
   Process: 17119 ExecStartPost=/bin/sleep 15 (code=exited, status=0/SUCCESS)
     Main PID: 17117 (python)
        Tasks: 6 (limit: 4657)
       Memory: 47.7M
      CGroup: /system.slice/panlsupervisor.service
              └─17117 /usr/bin/python /home/bridgetek/Projects/MRBS_Verification
                 └─17136 redis-server *:6379

Apr 09 15:27:55 administrator python[17117]: /home/bridgetek/Projects/MRBS_Ver
Apr 09 15:27:55 administrator python[17117]: ##### Started supervisor thr
Apr 09 15:27:55 administrator python[17117]: ##### http server is initiat
Apr 09 15:27:55 administrator python[17117]: * Serving Flask app "Supervisor"
Apr 09 15:27:55 administrator python[17117]: * Environment: production
Apr 09 15:27:55 administrator python[17117]: WARNING: Do not use the develop
Apr 09 15:27:55 administrator python[17117]: Use a production WSGI server in
Apr 09 15:27:55 administrator python[17117]: * Debug mode: off
Apr 09 15:27:55 administrator python[17117]: * Running on http://0.0.0.0:8081/
Apr 09 15:27:59 administrator systemd[1]: Started PanL Supervisor Service.
lines 1-21/21 (END)
```



**Note:** At any point of time, if any of the services are not starting, restart the respective services using the following command – `sudo systemctl restart <Service Name>`

## 4.4 SSL Certificate Setup

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.

## 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 room booking related activities.
Distribution Group for Users	Group (Users)	X	This group of users ( <b>prm-user-group</b> -<groupname>) are only allowed to access the following PRM components – <ul style="list-style-type: none"> <li>PRM Management Console</li> <li>Outlook Add Ins</li> <li>PanL PD100 Display device On spot booking</li> </ul>
Resource Account	Room Mailbox	X	This account will be part of the distribution group.
Distribution Group for Rooms	Group (Room List)	X	This group of rooms ( <b>prm-room-group</b> -<groupname>) are only recognized as valid resources in the PRM.
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"> <li>To communicate between PRM and Exchange Server.</li> <li>All the PRM Server / Room Booking related emails will be sent by this user</li> <li>Upon installation of PRM Server, this user account details must be added in the "<b>PRM Management Console</b> -&gt; <i>Settings</i> -&gt; <i>System</i>".</li> </ul>

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



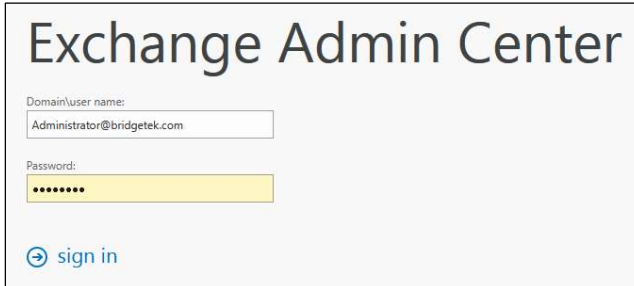
**Note:** Refer to the steps given under [Appendix > Exchange Server setup using Exchange Management Shell – Quick Reference](#) for more details.

### 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**

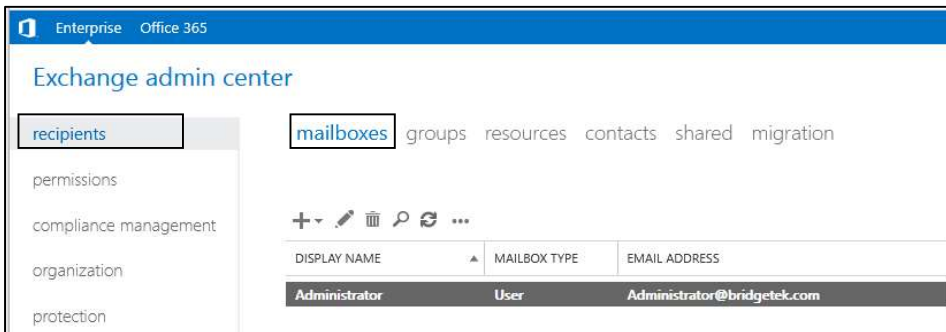
- Go to **https://<exchange servername>/ecp** and log in with Exchange Admin account.



The screenshot shows the Exchange Admin Center login page. It has a title "Exchange Admin Center" at the top. Below it, there are two input fields: "Domain\user name:" with the value "Administrator@bridgetek.com" and "Password:" with a masked password "\*\*\*\*\*". At the bottom left, there is a "sign in" button with a circular arrow icon.

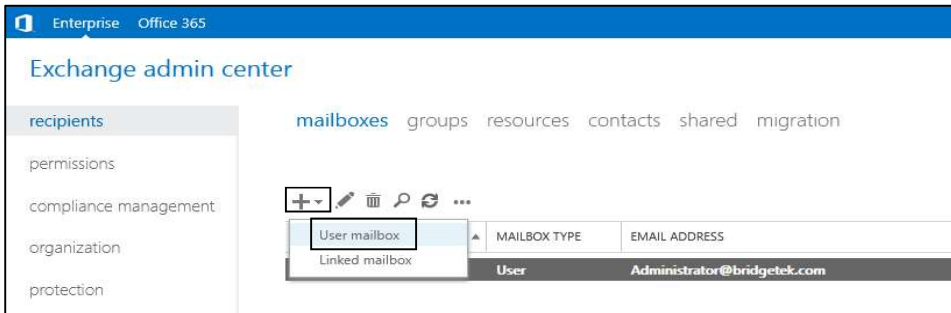
→ **Create Use Account**

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



The screenshot shows the Exchange Admin Center interface. The left sidebar has "recipients" selected. The main area shows "mailboxes" with a table of existing mailboxes. The table has columns "DISPLAY NAME", "MAILBOX TYPE", and "EMAIL ADDRESS". One entry is visible: "Administrator" with type "User" and email "Administrator@bridgetek.com". Above the table are icons for adding, editing, deleting, and other actions.

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



The screenshot shows the Exchange Admin Center interface with the "mailboxes" view. A dropdown menu is open from the "+" icon, showing "User mailbox" and "Linked mailbox". The "User mailbox" option is highlighted. The table below shows the same entry as the previous screenshot.

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

new user mailbox

Alias:  
User1

☐ Existing user

Browse...

☒ New user

First name:  
User1

Initials:

Last name:

\*Display name:  
User1

\*Name:  
User1

Organizational unit:  
 Browse...

\*User logon name:  
user1 @ @bridgetek.com

\*New password:  
.....

Save Cancel

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

Enterprise Office 365

Exchange admin center

recipients mailboxes groups resources contacts shared migration

permissions

compliance management

organization

protection

+ - ✎ 🗑️ 🔍 ↺ ...

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

## → Create Distribution Group for Users

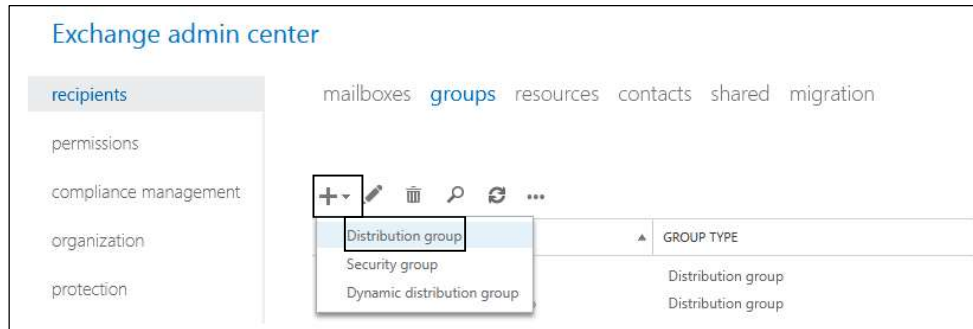
- Go to **"recipients"** → **"groups"**.

Exchange admin center

recipients mailboxes groups resources contacts shared migration

permissions

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



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

new distribution group

\*Display name:

\*Alias:

Notes:

Organizational unit:

\*Owners:  
+ -  

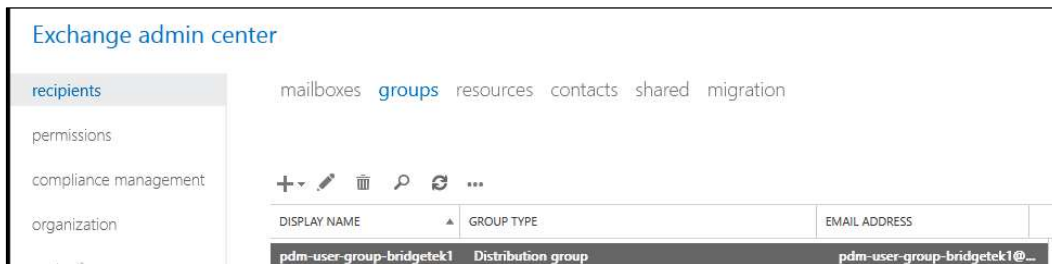
Administrator
<input type="text"/>

Members:  
☒ Add group owners as members  
+ -

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.  
☐ Choose whether the group is open to leave.

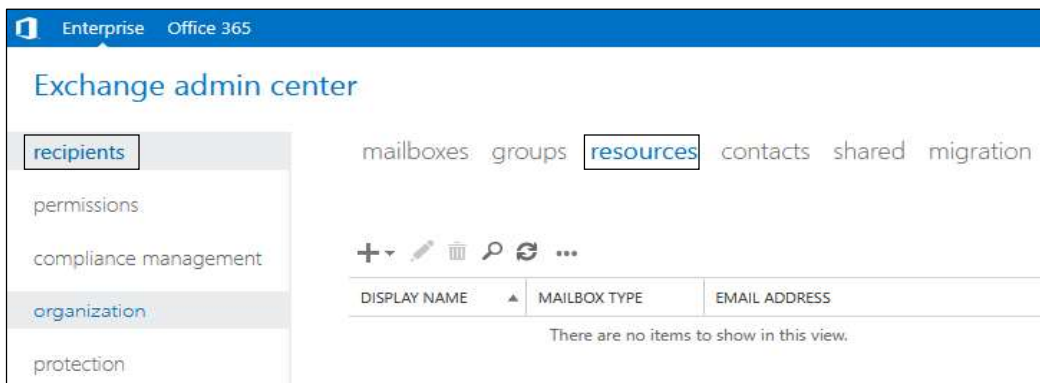


- The newly added distribution group is displayed. Add users to the newly created distribution group.

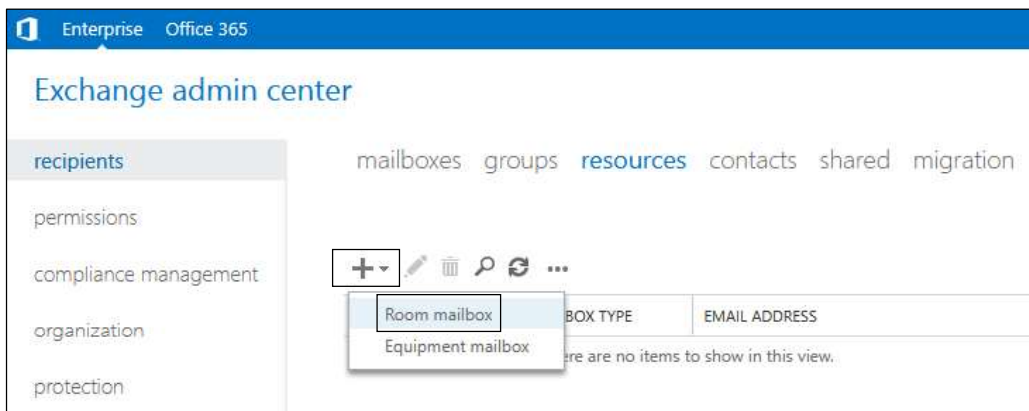


### → Create Room / Resource Account

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



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



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

new room mailbox

A room mailbox is a resource mailbox that's assigned to a physical location. Users can easily reserve rooms by including room mailboxes in meeting requests. Just select the room mailbox from the list and edit properties, such as booking requests or mailbox delegation. [Learn more](#)

\*Room name:

\*Alias:

Organizational unit:

Location:

Phone:

Capacity:

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

Exchange admin center

recipients

permissions

compliance management

organization

mailboxes groups **resources** contacts shared migration

+ - ✎ 🗑️ 🔍 🔄 ...

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Room1	Room	Room1@bridgetek.com

- Set room properties using the following command -

```
Set-CalendarProcessing -Identity "room1@bridgetek.com"
-MaximumDurationInMinutes 259200 -AutomateProcessing AutoAccept -
AllBookInPolicy $true -AllowConflicts $false -DeleteSubject $False -
AddOrganizerToSubject $False
```

## → Create Distribution Group for Rooms

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

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

```
New-DistributionGroup -Name "prm-room-group-bridgetek1" -RoomList
```

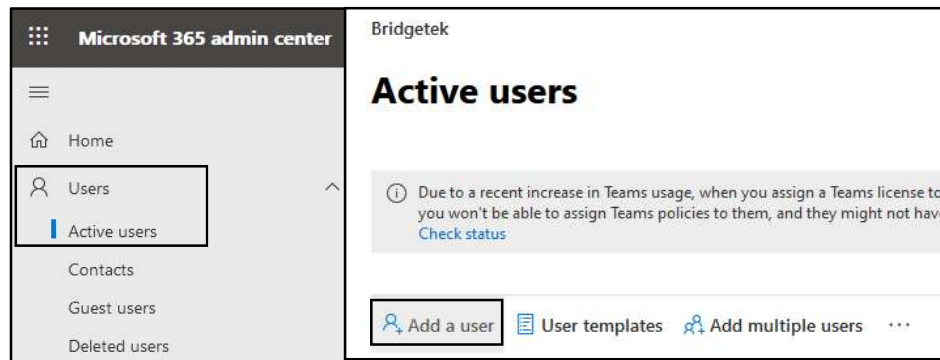


**Note:** A distribution group name should begin with prefix *prm-room-group* and be followed by the group name.

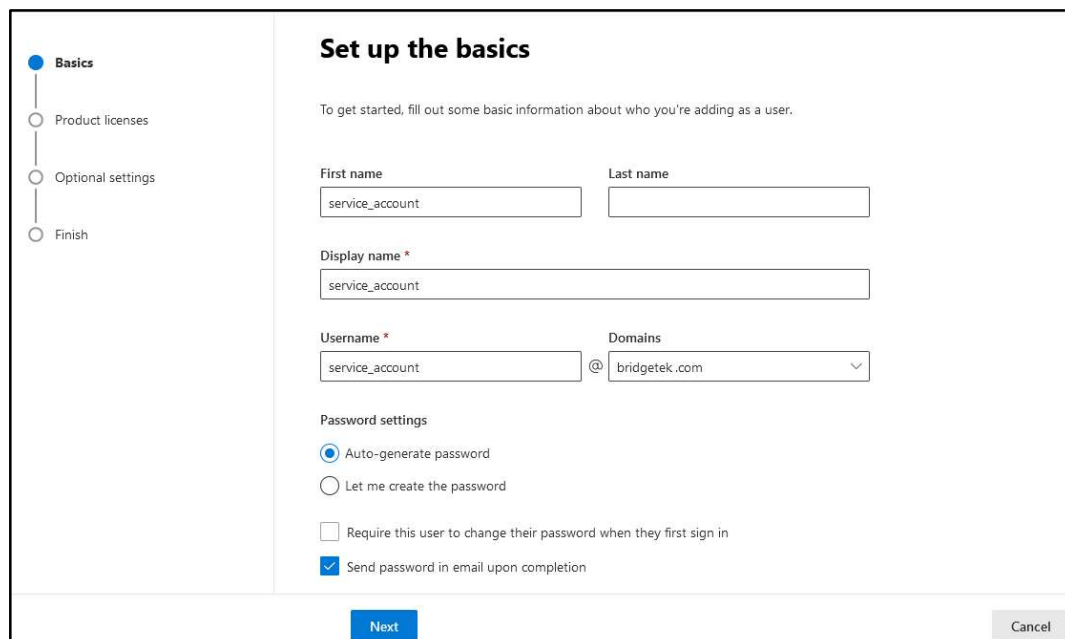
## → Create Impersonation User / Service Account & Grant Impersonation Rights

### Create User/Service Account

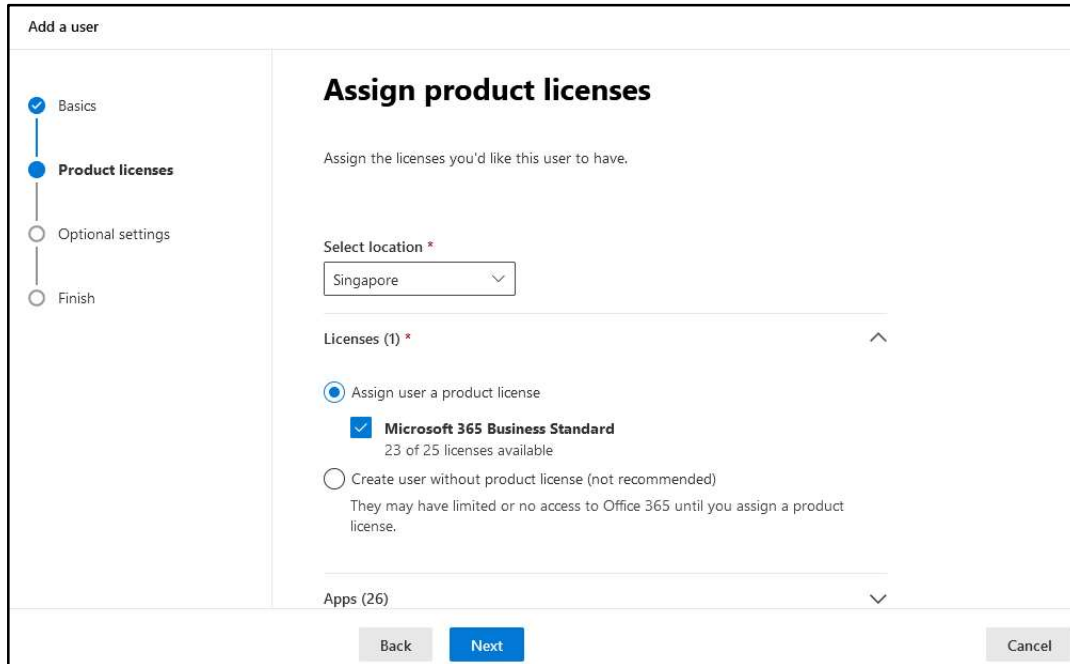
- In the Microsoft 365 admin centre, click "Users → Active Users → Add a user".



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



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



**Add a user**

Basics

**Product licenses**

Optional settings

Finish

### Assign product licenses

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

Select location \*

Singapore

Licenses (1) \*

☒ Assign user a product license

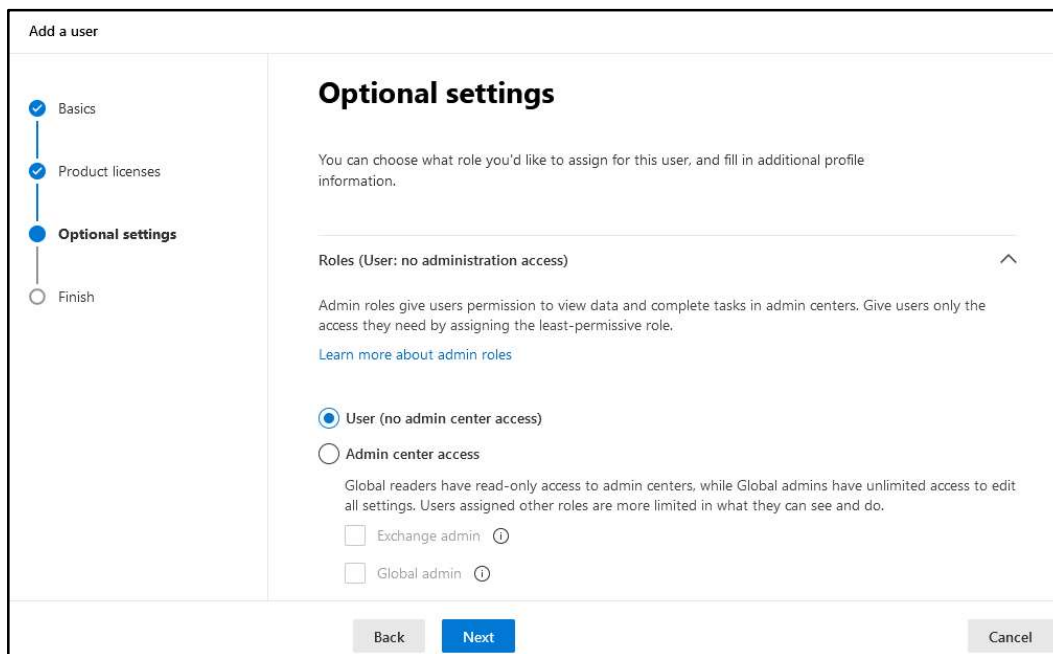
☒ **Microsoft 365 Business Standard**  
23 of 25 licenses available

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

Apps (26)

Back Next Cancel

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



**Add a user**

Basics

Product licenses

**Optional settings**

Finish

### Optional settings

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

Roles (User: no administration access)

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.  
[Learn more about admin roles](#)

☒ User (no admin center 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 ⓘ

☐ Global admin ⓘ

Back Next Cancel

- Verify the 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**

service\_account  
service\_account@bridgetek.com

[Edit](#)

**Password**

Type: Auto-generated  
Send To: Administrator@bridgetek.com

[Edit](#)

**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), 23 more

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

Add a user

✓ Basics

✓ Product licenses

✓ Optional settings

✓ Finish

✓

## service\_account added to active users

service\_account will now appear in your list of active users.

**User details**

Display name: service\_account  
Username: service\_account@bridgetek.com  
Password: Moq62307  
Sending to: Administrator@bridgetek.com

**Licenses bought**

None

**Licenses assigned**

Microsoft 365 Business Standard

Save these user settings as a template?

[Close](#)

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

Bridgetek

Dark mode

## Active users

Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. Until then, you won't be able to assign Teams policies to them, and they might not have access to some Teams features like calling and audio conferencing. [Check status](#)

Add a user
User templates
Add multiple users
...
Filter
Search

Display name ↑		Username	Licenses
Administrator Bridgetek	:	Administrator@bridgetek .com	Microsoft 365 Business Standard
Room1	:	Room1@bridgetek .com	Unlicensed
service_account	:	service_account@bridgetek .com	Microsoft 365 Business Standard

### → Granting Service Account Impersonation Rights

To grant the service account with impersonation permission for all accounts, refer to the steps given under section [Grant Service Acct Impersonation Right](#).



## 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 room booking related activities.
Distribution Group for Users	Group (Users)	X	<p>This group of users (<b>prm-user-group</b>-&lt;groupname&gt;) are only allowed to access the following PRM components –</p> <ul style="list-style-type: none"> <li>PRM Management Console</li> <li>Outlook Add Ins</li> <li>PD100 On spot booking</li> </ul>
Room Account	Room Mailbox	X	<p>This account's email addresses will be used –</p> <ul style="list-style-type: none"> <li>To book the rooms.</li> <li>This account will be part of the distribution group.</li> </ul>
Distribution Group for Rooms	Group (Room List)	X	<p>This group of rooms (<b>prm-room-group</b>-&lt;groupname&gt;) are only allowed to access the following PRM components –</p> <ul style="list-style-type: none"> <li>PRM Management Console</li> <li>Outlook Add Ins</li> <li>PD100 On spot booking</li> </ul>
Impersonation User / Service Account	User	1	<p>This user will be able to access multiple mailboxes and act as the mailbox owner. Impersonation is the best choice while dealing with multiple mailboxes because one can easily grant service account access to every mailbox in a database. This account will be used –</p> <ul style="list-style-type: none"> <li>To communicate between PRM and Exchange Server.</li> <li>All the PRM Server / Room Booking related emails will be sent by this user</li> <li>Upon installation of PRM Server, this user account details must be added in the "<b>PRM Management Console</b> -&gt; <i>Configuration</i> -&gt; <i>System</i>".</li> </ul> <p>Since large several emails are processed through this account, a dedicated account for this purpose is recommended.</p>

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



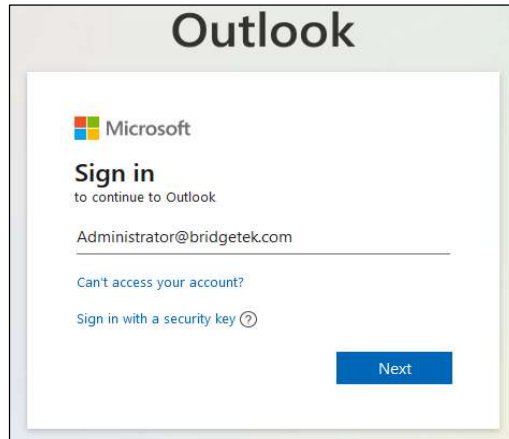
**Note:** Refer to the steps given under [Appendix > Microsoft 365 setup using Windows Powershell - Quick Reference](#) for more details.

## 5.2.1 Using Microsoft 365 Admin Center Console

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

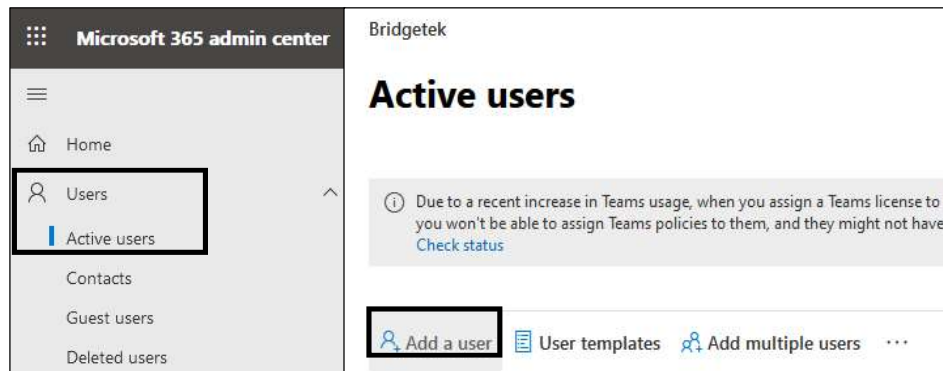
### → Login to Microsoft 365 Admin Center Console

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

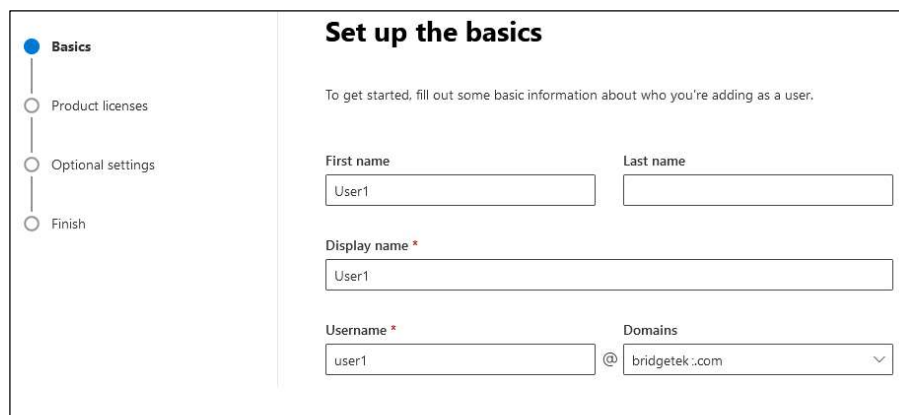


### → Create User Account

- 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

✓ Basics

● **Product licenses**

○ Optional settings

○ Finish

## Assign product licenses

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

Select location \*

Singapore

Licenses (1) \*

☒ 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

✓ Basics

✓ Product licenses

● **Optional settings**

○ Finish

## Optional settings

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

Roles (User: no administration access)

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

[Learn more about admin roles](#)

☒ **User (no admin center 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 ⓘ

☐ Global admin ⓘ

☐ Global reader ⓘ

☐ Helpdesk admin ⓘ

☐ Service support admin ⓘ

Back

Next

Cancel

- 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@bridgetek.com  
[Edit](#)

**Password**

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

**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), 23 more  
[Edit](#)

**Roles (default)**

User (no admin center 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@bridgetek.com  
Password: \*\*\*\*\* [Show](#)  
Sending to: Administrator@bridgetek.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 domain, password, product licenses, and roles.  
[Review settings for this user template](#)

[Close](#)

The user account details are added to active users list.

Bridgetek

Dark mode

## Active users

Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. Until then, you won't be able to assign Teams policies to them, and they might not have access to some Teams features like calling and audio conferencing. [Check status](#)

Add a user
User templates
Add multiple users
...
Filter
Search

Display name ↑		Username	Licenses
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 **"Teams & groups"** → **"Active teams & groups"**. Click **"Add a group"** and select **"Distribution"**. Click **[Next]**.

Microsoft 365 admin center

Search

Home

Users

Teams & groups

Active teams & groups

Policies

Deleted groups

Shared mailboxes

Roles

Resources

Billing

Home > Active teams & groups

Active teams and groups

Microsoft Teams supports collaboration through chat, calls, and online meetings. The teams you add are collections of people, content, and tools. Groups are a collection of people, and are useful if you only need a group email address. It can take up to an hour for new distribution groups and mail-enabled security groups to appear here. To see them immediately, [go to Exchange admin center](#).

[Learn about Microsoft Teams](#)

Microsoft 365

Distribution list

Mail-enabled security

Security

Add a group

Export

Refresh

Microsoft 365 admin center

Search

Home

Users

Teams & groups

Active teams & groups

Policies

Deleted groups

Shared mailboxes

Roles

Resources

Billing

Support

Settings

Setup

Reports

Health

Admin centers

Active teams and groups > Add a group

Group type

Basics

Owners

Members

Settings

Finish

Choose a group type

Choose the group type that best meets your team's needs. [Learn more about group types](#)

☐ Microsoft 365 (recommended)  
Creates a group email to collaborate. You can also add Microsoft Teams for group conversations, files, and calendars.

☒ Distribution  
Creates an email address for a group of people.

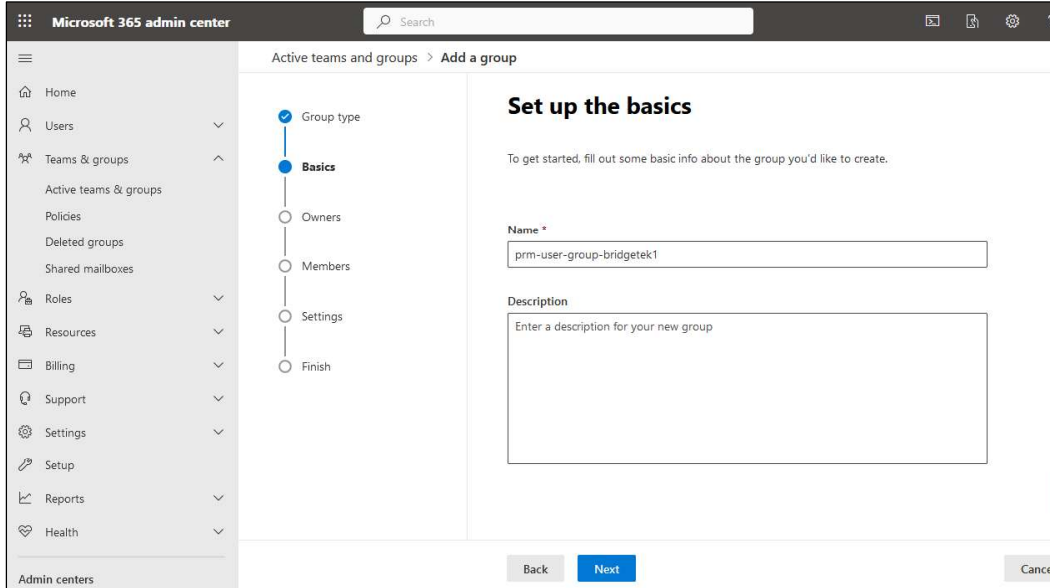
☐ Mail-enabled security  
A distribution list that can also be used to control access to OneDrive and SharePoint.

☐ Security  
Controls access to OneDrive and SharePoint and can be used for Mobile Device Management for Microsoft 365.

Next

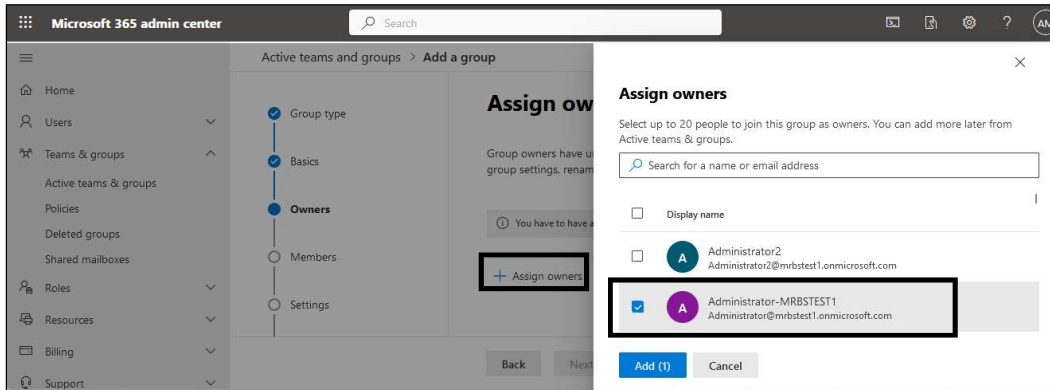
Cancel

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



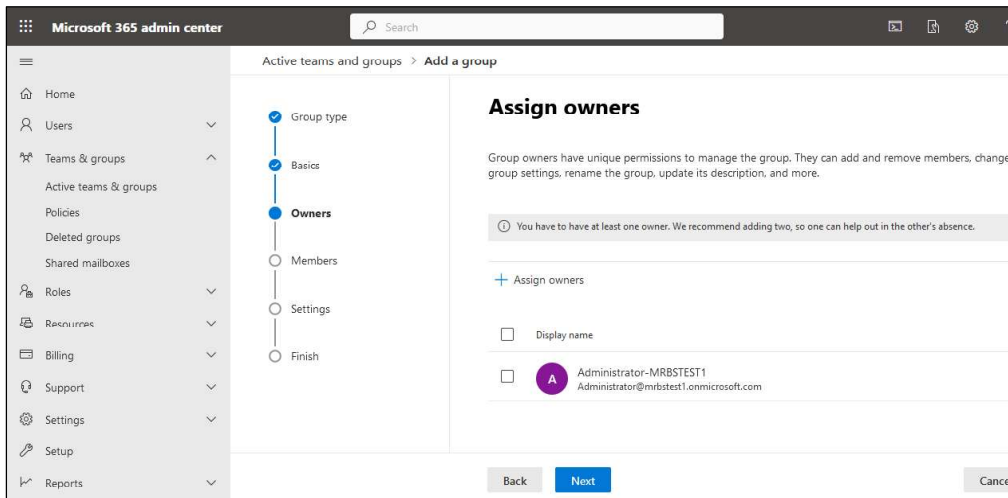
The screenshot shows the 'Microsoft 365 admin center' interface. The left sidebar contains navigation links: Home, Users, Teams & groups, Active teams & groups, Policies, Deleted groups, Shared mailboxes, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. The main content area is titled 'Active teams and groups > Add a group'. A progress bar on the left indicates the steps: Group type (selected), Basics (current), Owners, Members, Settings, and Finish. The 'Set up the basics' section contains a 'Name' field with the value 'prm-user-group-bridgetek1' and a 'Description' field with the placeholder text 'Enter a description for your new group'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

- Assign Owners** Click **+ Assign Owners** and select the owners from the list. Click **[Add]**.



The screenshot shows the 'Microsoft 365 admin center' interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Active teams and groups > Add a group'. The progress bar indicates the steps: Group type, Basics, Owners (current), Members, Settings, and Finish. The 'Assign owners' section contains a search bar with the placeholder text 'Search for a name or email address'. Below the search bar, there is a list of users. The first user is 'Administrator2' with email 'Administrator2@mrbtest1.onmicrosoft.com'. The second user is 'Administrator-MRBTEST1' with email 'Administrator@mrbtest1.onmicrosoft.com'. The second user is selected, indicated by a blue checkmark. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

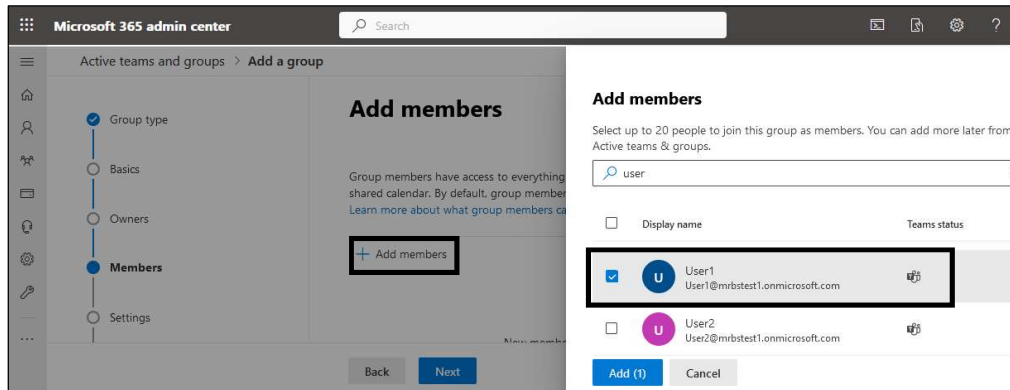
- The newly added owner details are displayed. Click **[Next]**.



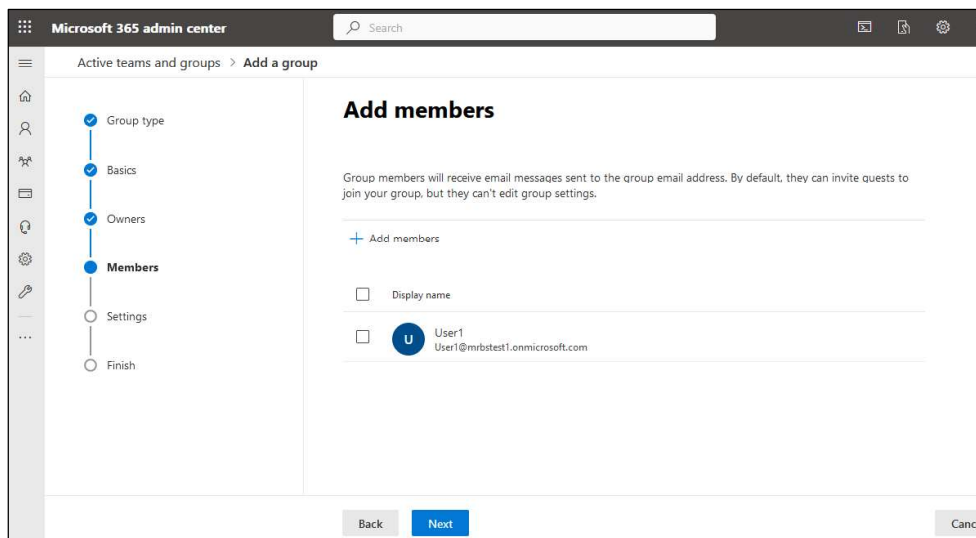
The screenshot shows the 'Microsoft 365 admin center' interface. The left sidebar is the same as the previous screenshots. The main content area is titled 'Active teams and groups > Add a group'. The progress bar indicates the steps: Group type, Basics, Owners (current), Members, Settings, and Finish. The 'Assign owners' section contains a message: 'Group owners have unique permissions to manage the group. They can add and remove members, change group settings, rename the group, update its description, and more.' Below this, there is a warning: 'You have to have at least one owner. We recommend adding two, so one can help out in the other's absence.' Below the warning, there is a '+ Assign owners' button. Below the button, there is a list of users. The first user is 'Administrator-MRBTEST1' with email 'Administrator@mrbtest1.onmicrosoft.com'. The user is selected, indicated by a blue checkmark. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.



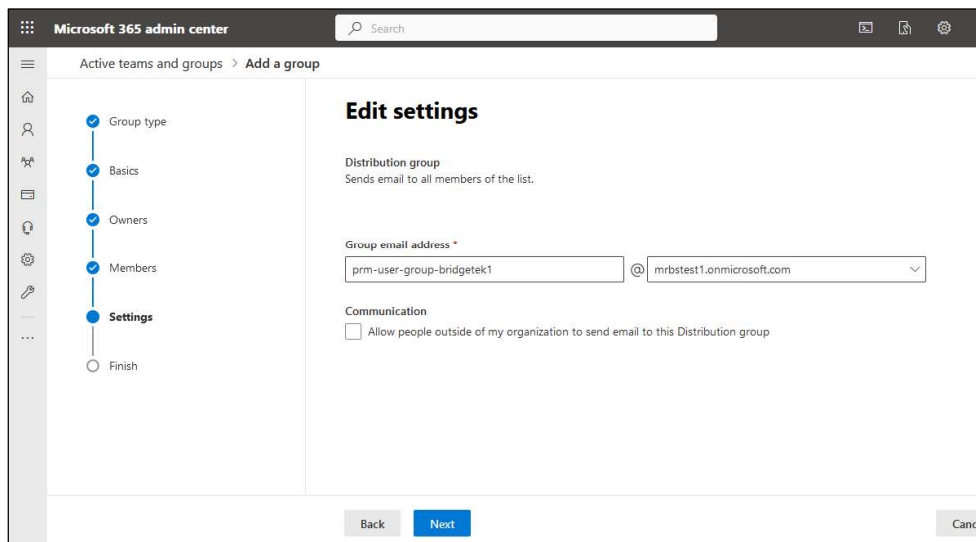
- **Add Members** Click **+ Add members** and select the member(s) from the list.



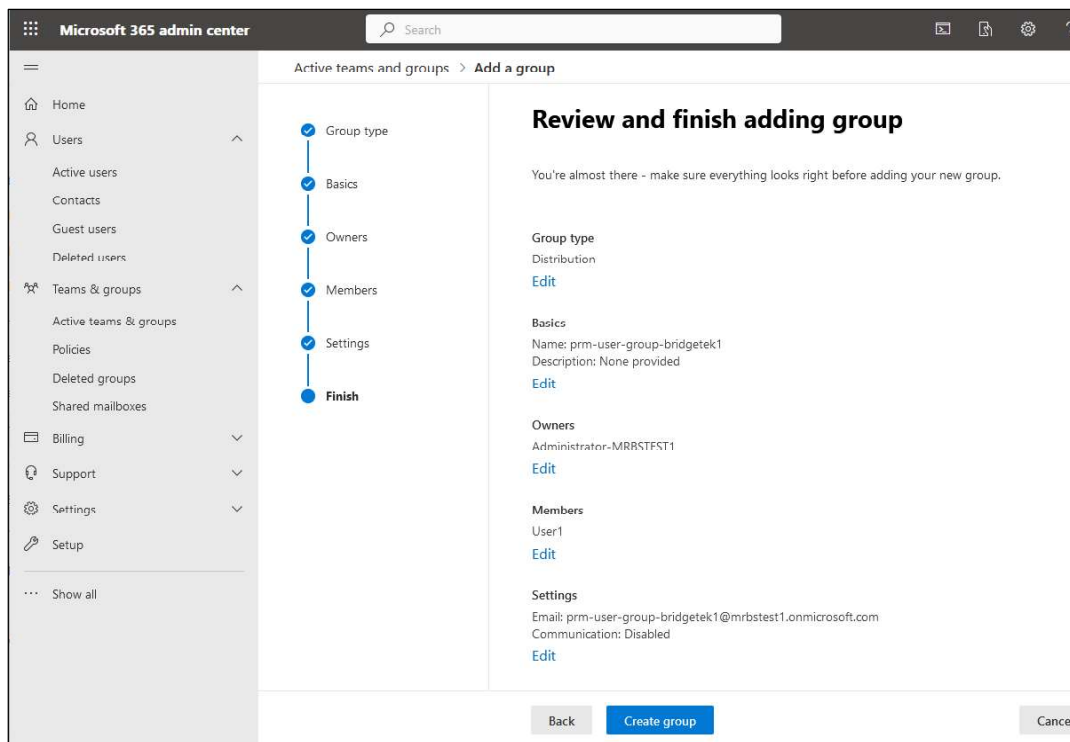
- Click **[Add]**. The newly added member details are displayed. Click **[Next]**.



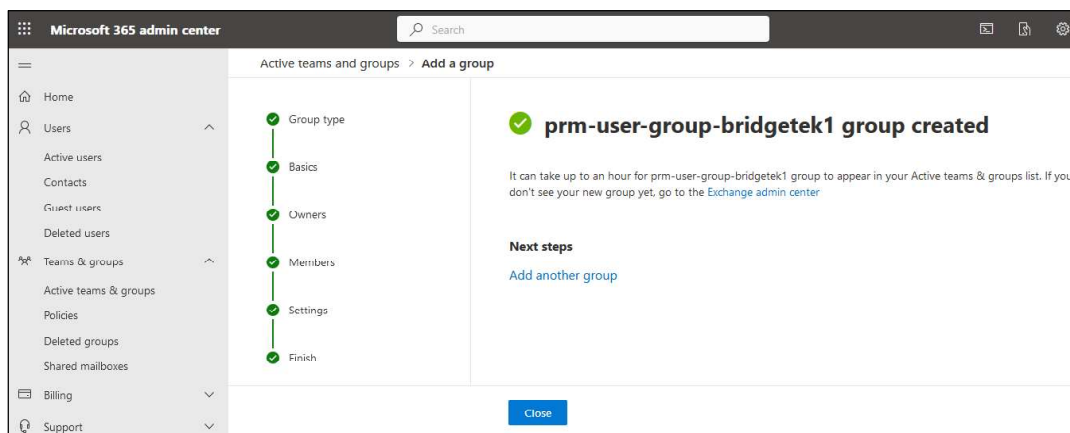
- **Edit Settings** Modify the settings as required and click **[Next]**.



- Review and finish adding group – upon reviewing, click **[Create group]**.

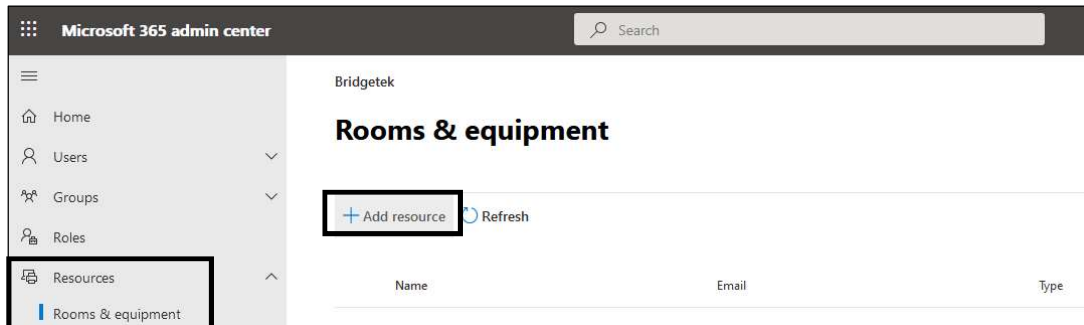


- Upon clicking create group, an appropriate message indicating that the group has been created, is displayed.



## → Create Room / 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 \*

Room1

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

Email \*

Room1

@

Domains

mrtest1.onmicrosoft.com

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

Capacity

10

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

Location

SG-03-05

Save

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

×

✓

Room1 is ready

You've created a new mailbox for your Room and can now use the email address to book the resource.

Default booking options have been applied, such as allowing repeating meetings and automatically accepting meeting invites. You can change these at any time.

**Next Steps**

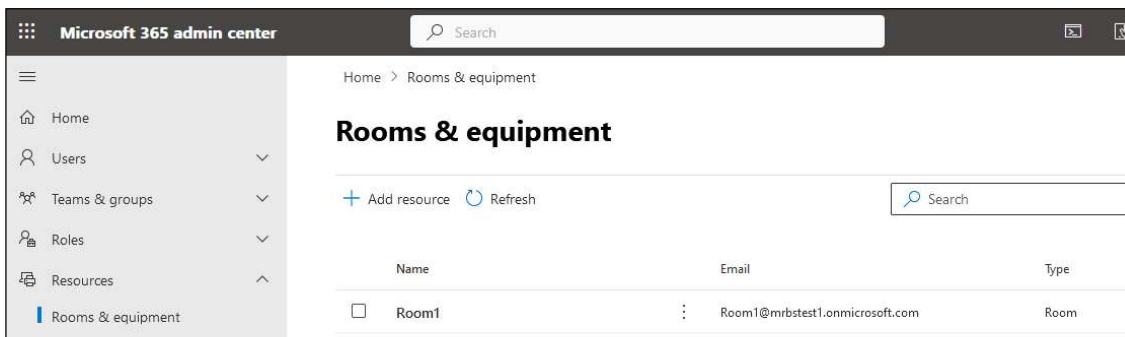
[Edit booking options](#)

[Add another resource](#)

**Learn more**

[Use the Scheduling Assistant in Outlook to add rooms to meetings](#)

[Working with rooms and equipment](#)



- Set room properties using the following command –

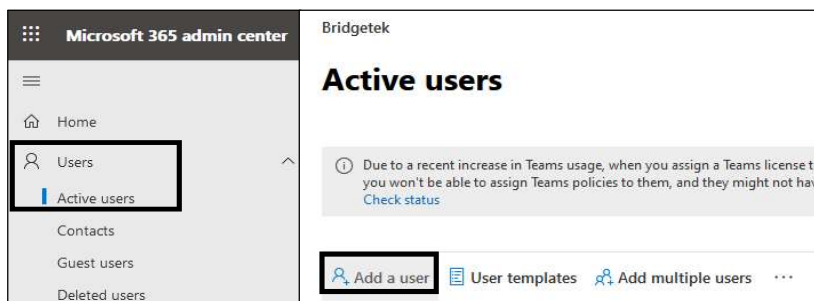
```
Set-CalendarProcessing -Identity "room1@bridgetek.com" -
ScheduleOnlyDuringWorkHours $true -MaximumDurationInMinutes 259200 -
AutomateProcessing AutoAccept -AllBookInPolicy $true -AllowConflicts $false
-DeleteSubject $False -AddOrganizerToSubject $False
```

### → Create Distribution Group for Rooms

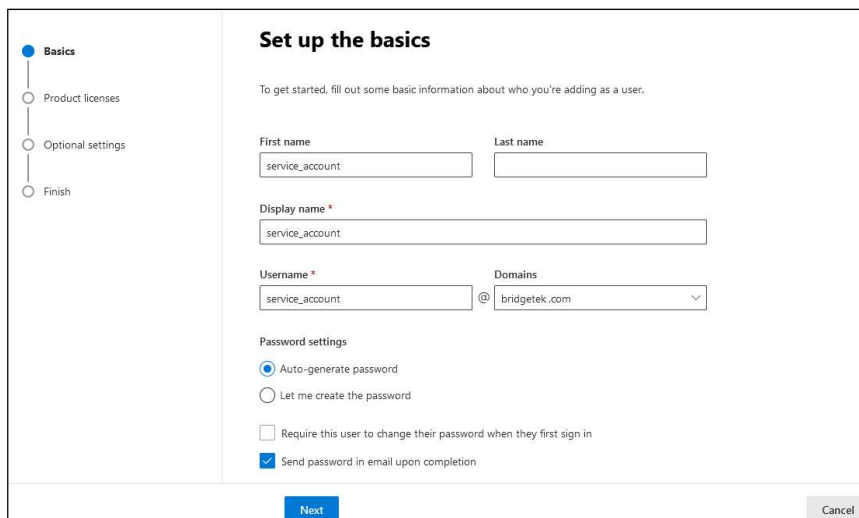
The distribution group for Rooms (RoomList) can be created **only** using the [Exchange PowerShell](#).

### → Create Impersonation User / Service Account

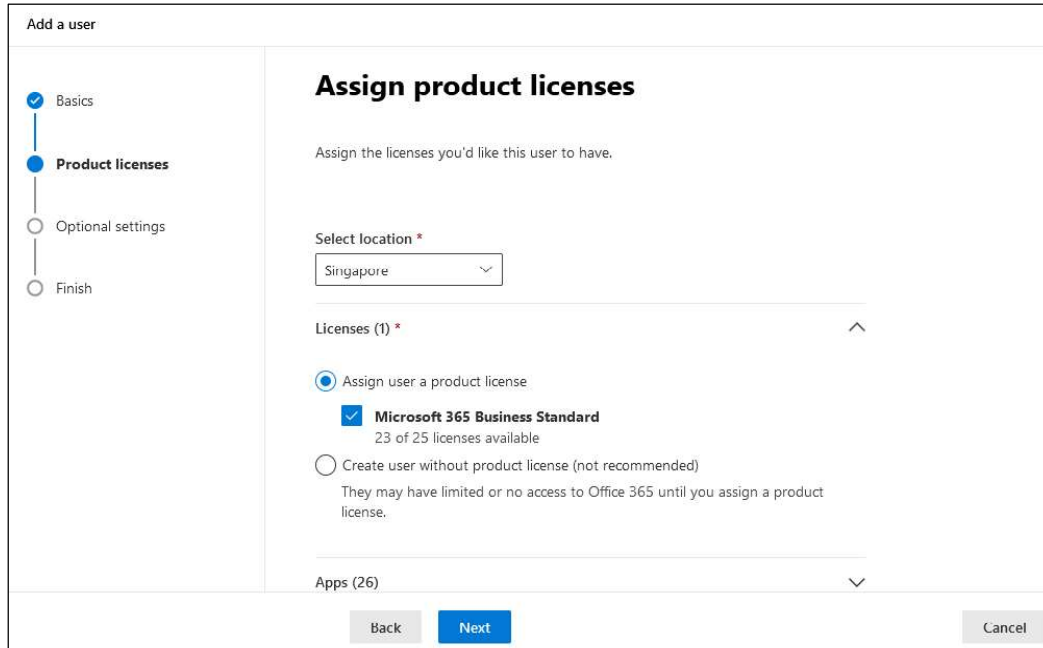
- In the Microsoft 365 admin centre, click “Users → Active Users → Add a user”.



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

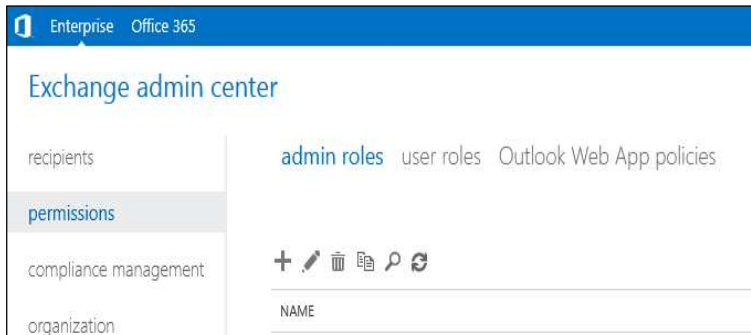


- Assign the “**product licenses**”. Click [**Next**].



The screenshot shows the 'Add a user' wizard with the 'Product licenses' step selected. The left sidebar shows the progress: Basics (checked), Product licenses (selected), Optional settings, and Finish. The main area is titled 'Assign product licenses' and contains 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 'Licenses (1) \*', there are two options: 'Assign user a product license' (selected) and 'Create user without product license (not recommended)'. Under the selected option, 'Microsoft 365 Business Standard' is checked, with '23 of 25 licenses available' shown below it. At the bottom, there is an 'Apps (26)' dropdown menu and three buttons: 'Back', 'Next', and 'Cancel'.

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



The screenshot shows the Exchange admin center interface. The top bar has 'Enterprise' and 'Office 365' tabs. The main header is 'Exchange admin center'. Below the header, there is a sidebar with links: recipients, permissions (selected), compliance management, and organization. The main content area has tabs for 'admin roles', 'user roles', and 'Outlook Web App policies'. Below the tabs, there are icons for adding, editing, deleting, and searching, followed by a search bar labeled 'NAME'.

- Verify the 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**  
service\_account  
service\_account@bridgetek .com  
[Edit](#)

**Password**  
Type: Auto-generated  
Send To: Administrator@bridgetek .com  
[Edit](#)

**Product licenses**  
Location: Singapore  
Licenses: Microsoft 365 Business Standard  
Apps: Power Virtual Agents for Office 365  
more

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


**service\_account added to active users**

service\_account will now appear in your list of active users.

**User details**  
Display name: service\_account  
Username: service\_account@bridgetek.com  
Password: Moq62307  
Sending to: Administrator@bridgetek.com

**Licenses bought**  
None

**Licenses assigned**  
Microsoft 365 Business Standard

[Save these user settings as a template?](#)

[Close](#)

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

Bridgetek

Dark mode

### Active users

Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. Until then, you won't be able to assign Teams policies to them, and they might not have access to some Teams features like calling and audio conferencing. [Check status](#)

Add a user
User templates
Add multiple users
...

Filter
Search

Display name ↑	Username	Licenses
Administrator Bridgetek	Administrator@bridgetek .com	Microsoft 365 Business Standard
Room1	Room1@bridgetek .com	Unlicensed
service_account	service_account@bridgetek .com	Microsoft 365 Business Standard

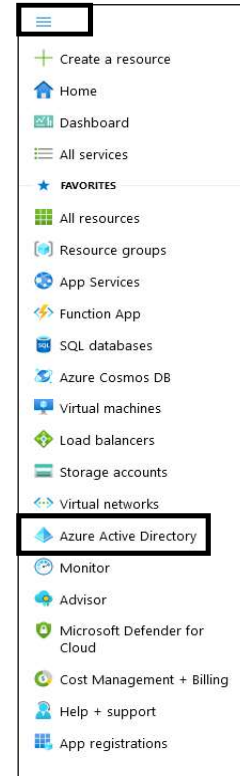
### → Granting Service Account Impersonation Rights

Refer to the steps given under section [Grant Service Account Impersonation Rights](#).



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

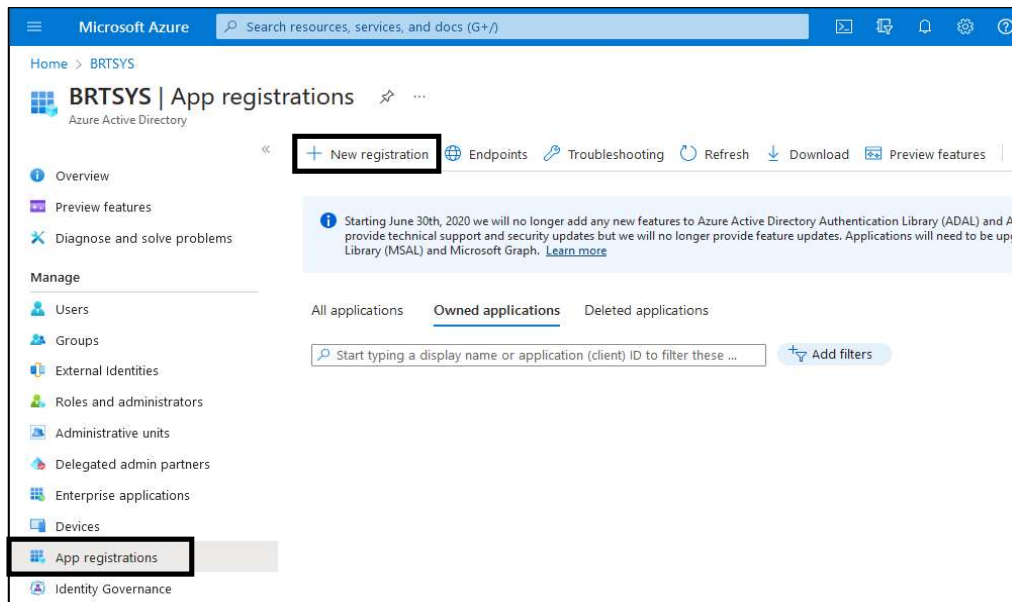
- Access Azure Portal using the administrator account - <https://portal.azure.com>
- Go to **Azure Active Directory** from the left navigation menu.
  - Register Applications
  - Setup Authentication (Redirect URI)
  - Setup Client Secret
  - Setup API Permissions



### 5.2.2.1 PRM Client

#### 5.2.2.1.1 App Registration

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



- Enter the **Application name** – *PRM Client Credentials*; select the **Supported account types** – *Accounts in this organization 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).

PRM Client Credentials

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (BRTSYS 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...](#)

**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 organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

- The PRM Client Credentials application is successfully created.

Home > App registrations >

## PRM Client Credentials

Search « 🗑️ Delete 🌐 Endpoints 🔍 Preview features

**Overview**

Quickstart

Integration assistant

**Manage**

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

**Essentials**

Display name : [PRM Client Credentials](#)

Application (client) ID : fe02552f-0546-45bb-914f-20e81df6c974

Object ID : 76f7bdf1-cdf0-40b0-b542-f794ec9d7367

Directory (tenant) ID : 92ec9fe9-20d5-4eb7-936d-2a60790cb9dd

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

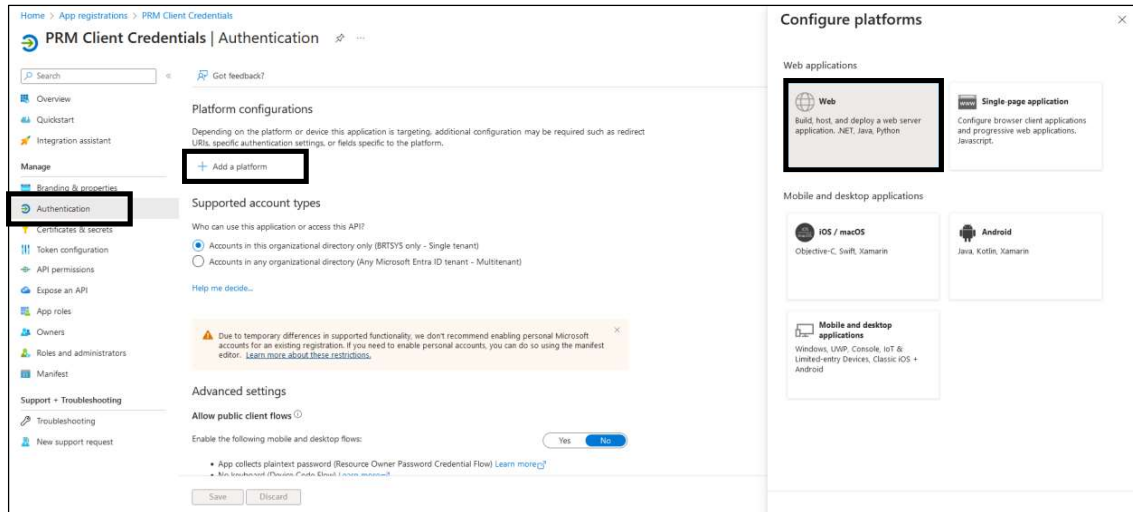
Application ID URI : [Add an Application ID URI](#)

Managed application in lo... : [PRM Client Credentials](#)

**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://prm.prm.local/auth/oidc-login>
- Enter the **Front-channel logout URL** – PRM Front-channel Logout URI (<https://prm.prm.local/api/oidc-logout>). This field is needed only when implementing single sign on. **(Mandatory)**.

prm.local - indicates the domain name.

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

Configure Web

[All platforms](#)
[Quickstart](#)
[Docs](#)

\* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#)

Select the tokens you would like to be issued by the authorization endpoint:

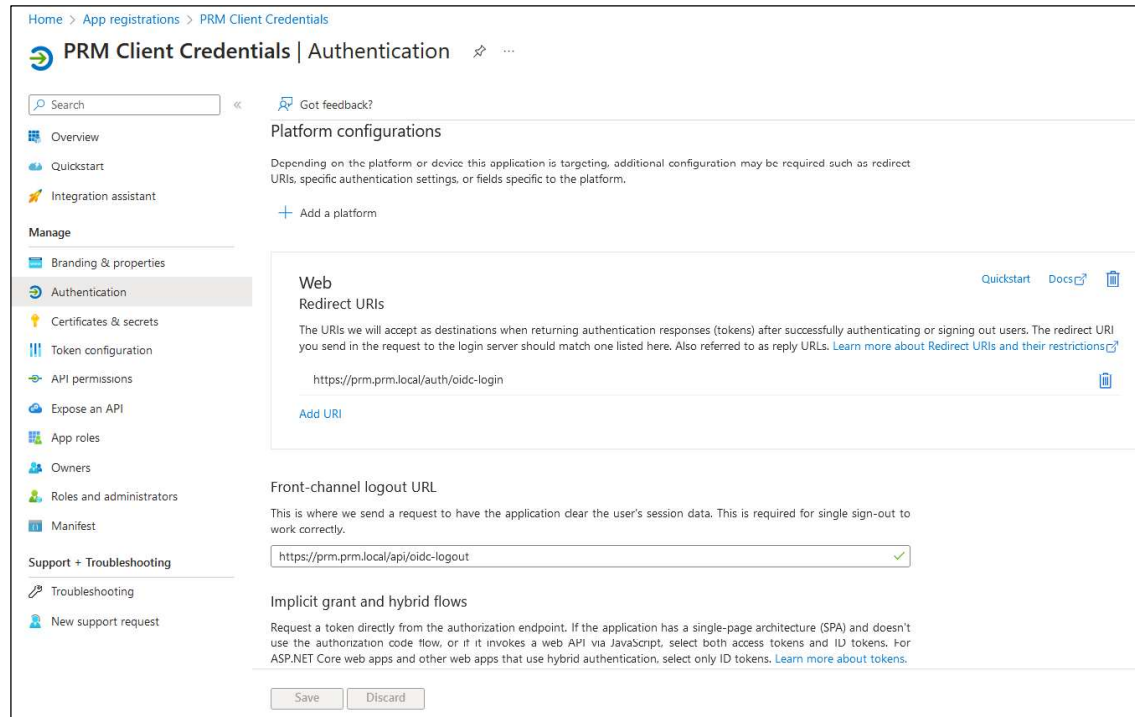
☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Configure

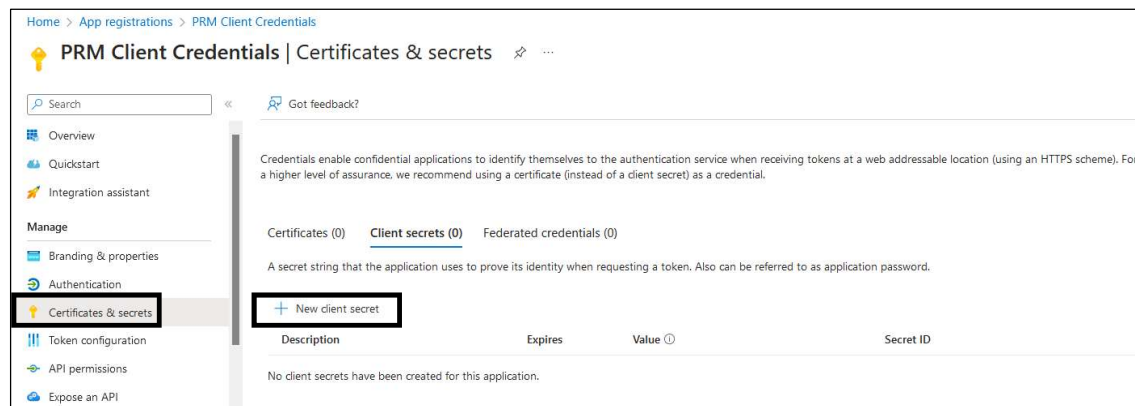
Cancel

→ The configuration details are displayed.

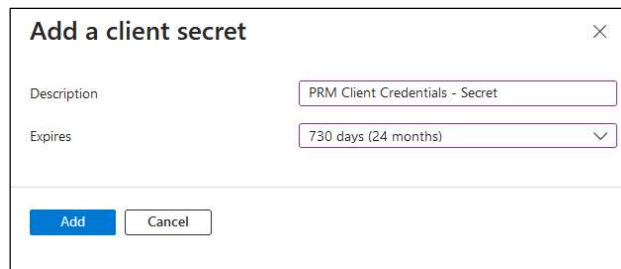


### 5.2.2.1.3 Setup Client Secret

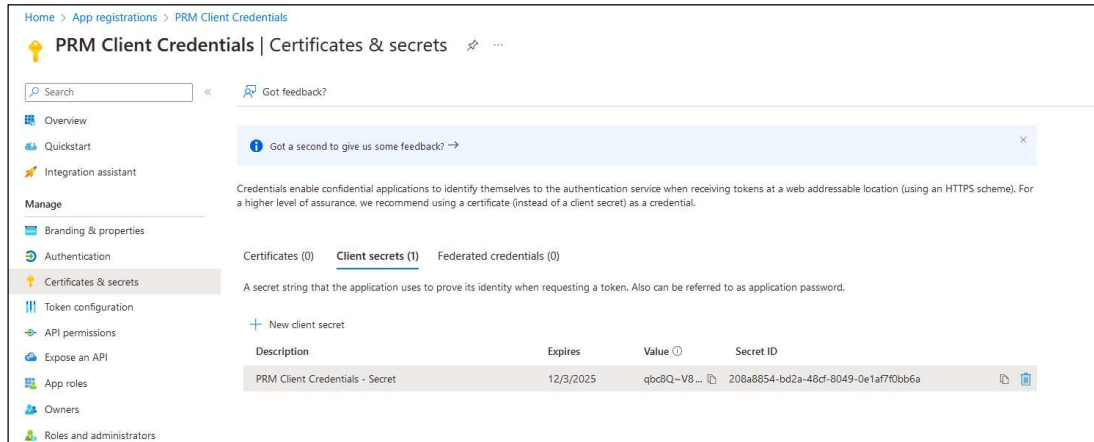
→ In the left menu, select **Certificates & secrets**; click **+ New client secret**.



→ 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.



Home > App registrations > PRM Client Credentials

PRM Client Credentials | Certificates & secrets

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates (0) Client secrets (1) Federated credentials (0)

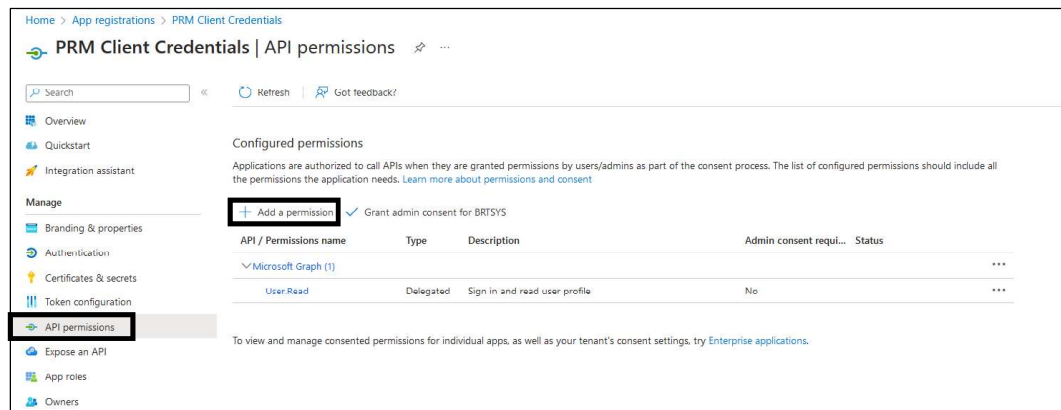
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
PRM Client Credentials - Secret	12/3/2025	qbc8Q-V8...	208a8854-bd2a-48cf-8049-0e1af7f0bb6a

#### 5.2.2.1.4 Setup API Permissions

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



Home > App registrations > PRM Client Credentials

PRM Client Credentials | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins 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](#)

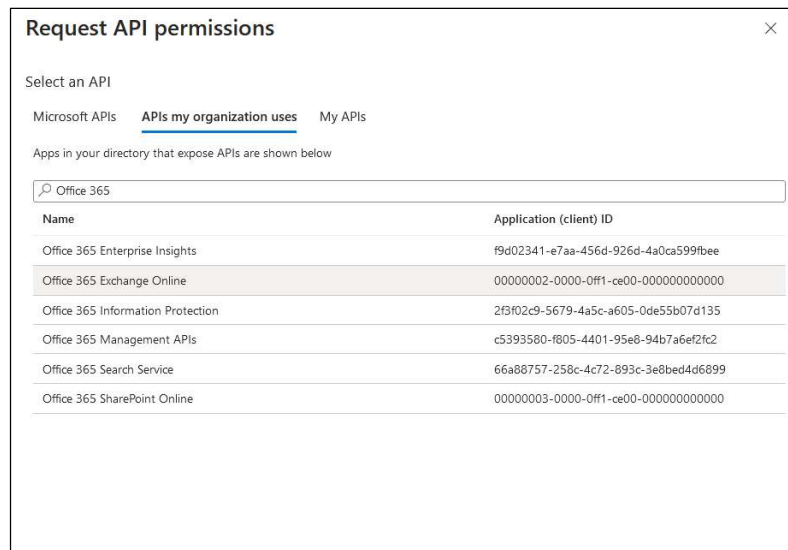
+ Add a permission

Grant admin consent for BRTSYS

API / Permissions name	Type	Description	Admin consent requi...	Status
Microsoft Graph (1)				...
User Read	Delegated	Sign in and read user profile	No	...

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

- 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.



Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

Office 365

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 Search Service	66a88757-258c-4c72-893c-3e8bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000

→ Click **Application permissions**; Check **full\_access\_as\_app**; Click **Add permissions**.

Request API permissions

[All APIs](#)

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

PermissionAdmin consent required

Permissions (1)

☒

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.

Home > App registrations > PRM Client Credentials

PRM Client Credentials | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

+

Add a permission

✓ Grant admin consent for BRTSYS

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins 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.](#)

API / Permissions name	Type	Description	Admin consent requi...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange Online (1)				...
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	⚠ Not granted for BRTSYS

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [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.

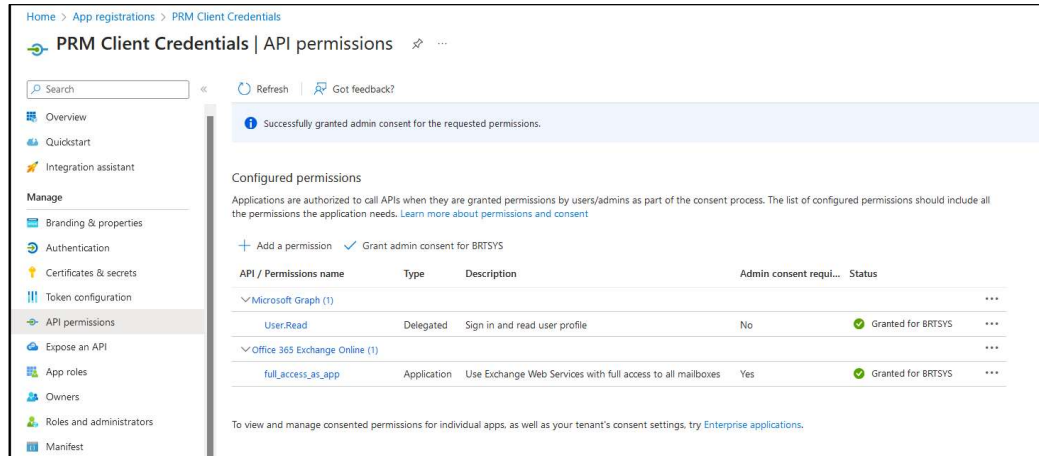
Yes

No

[Product Page](#)  
[Document Feedback](#)

38  
Copyright © BRT Systems Pte Ltd

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



Home > App registrations > PRM Client Credentials

PRM Client Credentials | API permissions

Search Refresh Got feedback?

Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins 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 Grant admin consent for BRTSYS

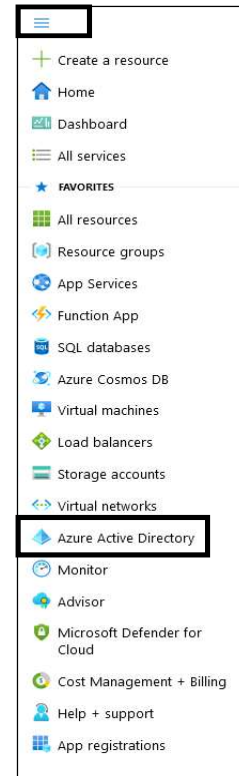
API / Permissions name	Type	Description	Admin consent requi...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	Granted for BRTSYS
Office 365 Exchange Online (1)				...
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	Granted for BRTSYS

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



### 5.2.3 Modern Authentication using OAuth 2.0 - ROPC

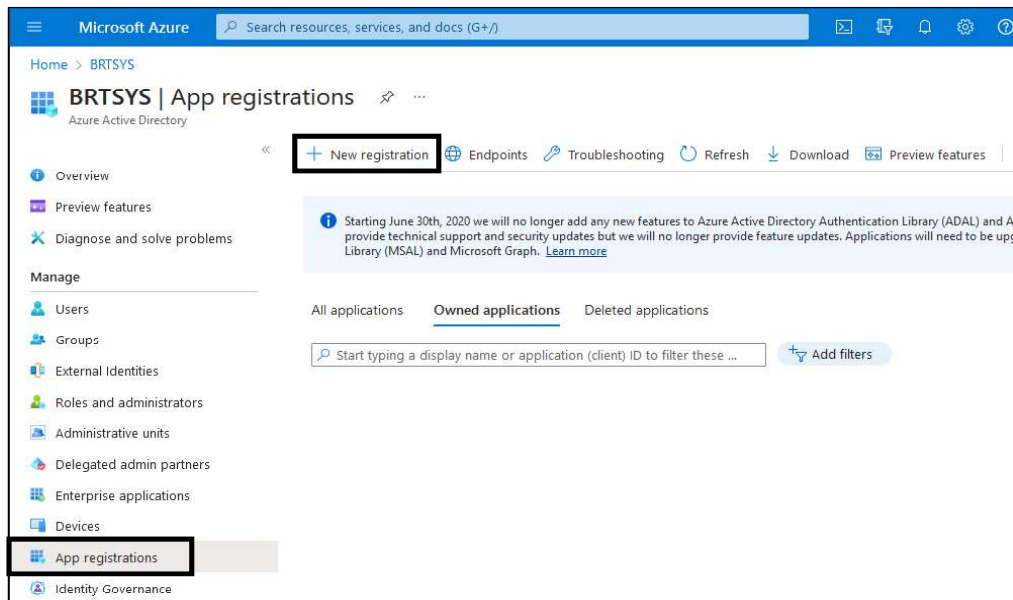
- Access Azure Portal using the administrator account – <https://portal.azure.com>.
- Go to **Azure Active Directory** from the left navigation menu.



#### 5.2.3.1 PRM Client

##### 5.2.3.1.1 App Registration

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



- Enter the **Application name** – *PRM ROPC*; select the **Supported account types** – *Accounts in this organization 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).

PRM ROPC

**Supported account types**

Who can use this application or access this API?

☒ Accounts in this organizational directory only (BRTSYS 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...](#)

**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 organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

- The PRM ROPC application is successfully created.

Home > App registrations >

## PRM ROPC

Search  Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

**Essentials**

Display name : [PRM ROPC](#)

Application (client) ID : 6a575758-3577-4aec-b51b-4fa90513e546

Object ID : d02fcb07-6f0c-42ed-8fac-2177e3d0cccf

Directory (tenant) ID : 92ec9fe9-20d5-4eb7-936d-2a60790cb9dd

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

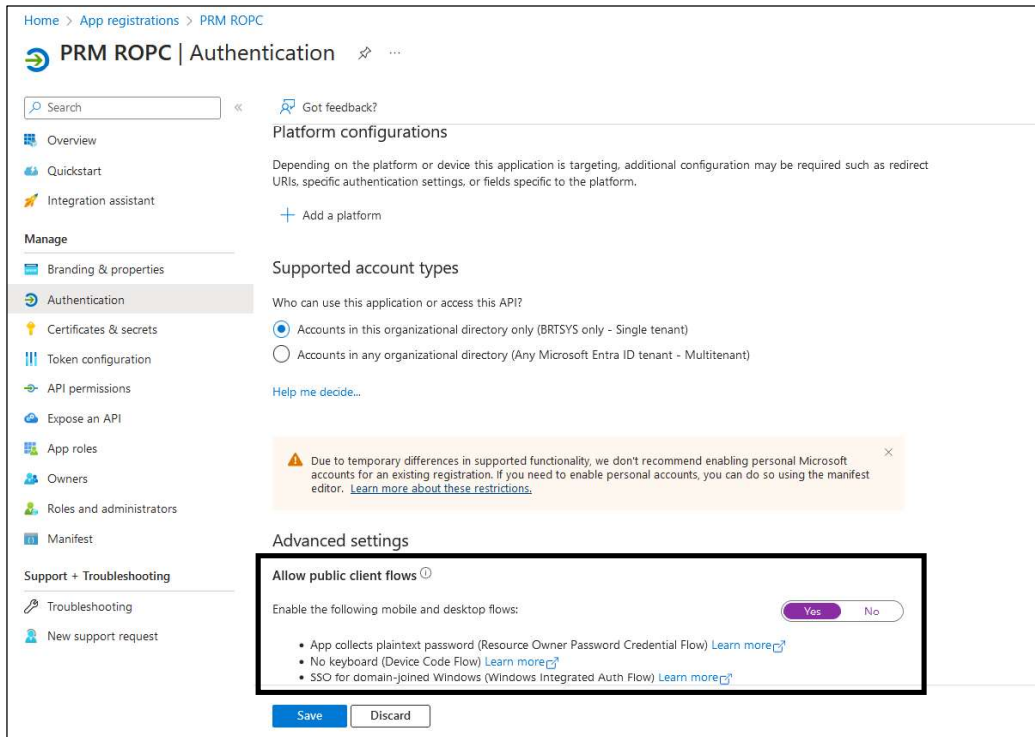
Application ID URI : [Add an Application ID URI](#)

Managed application in lo... : [PRM ROPC](#)

**Get Started** Documentation

### 5.2.3.1.2 Setup Authentication

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



Home > App registrations > PRM ROPC

PRM ROPC | Authentication

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

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

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

[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

☒ App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)

☒ No keyboard (Device Code Flow) [Learn more](#)

☒ SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

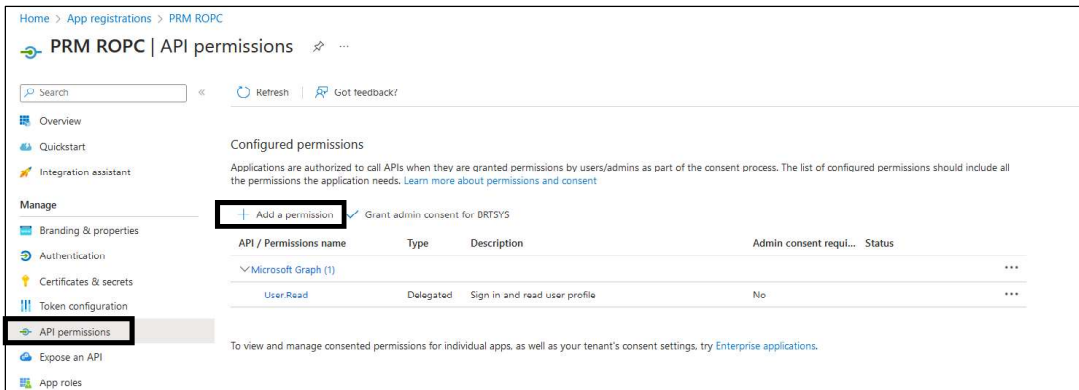
Yes No

Save Discard

→ Click **[Save]**.

### 5.2.3.1.3 Setup API Permissions

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



Home > App registrations > PRM ROPC

PRM ROPC | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins 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](#)

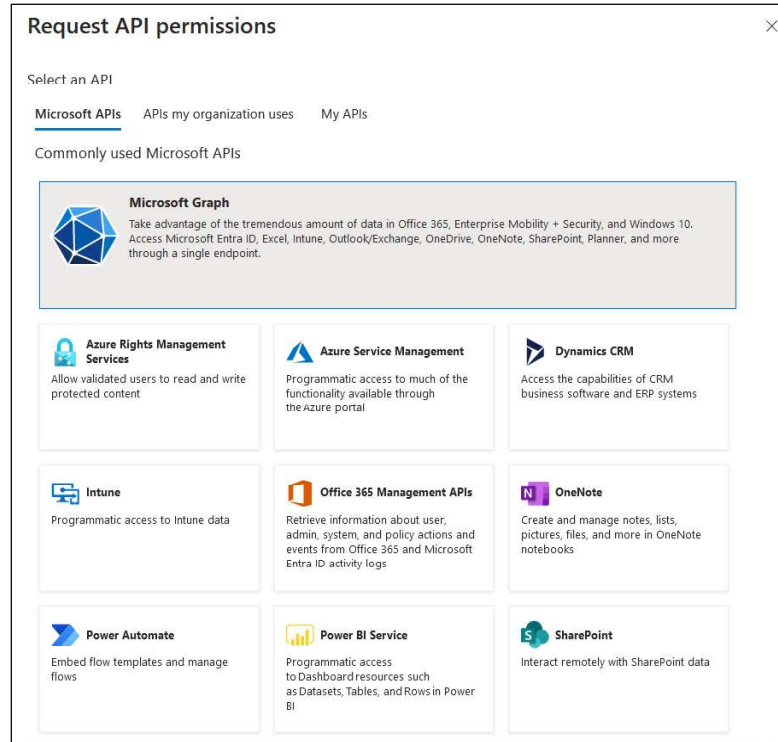
+ Add a permission

Grant admin consent for BRTSYS

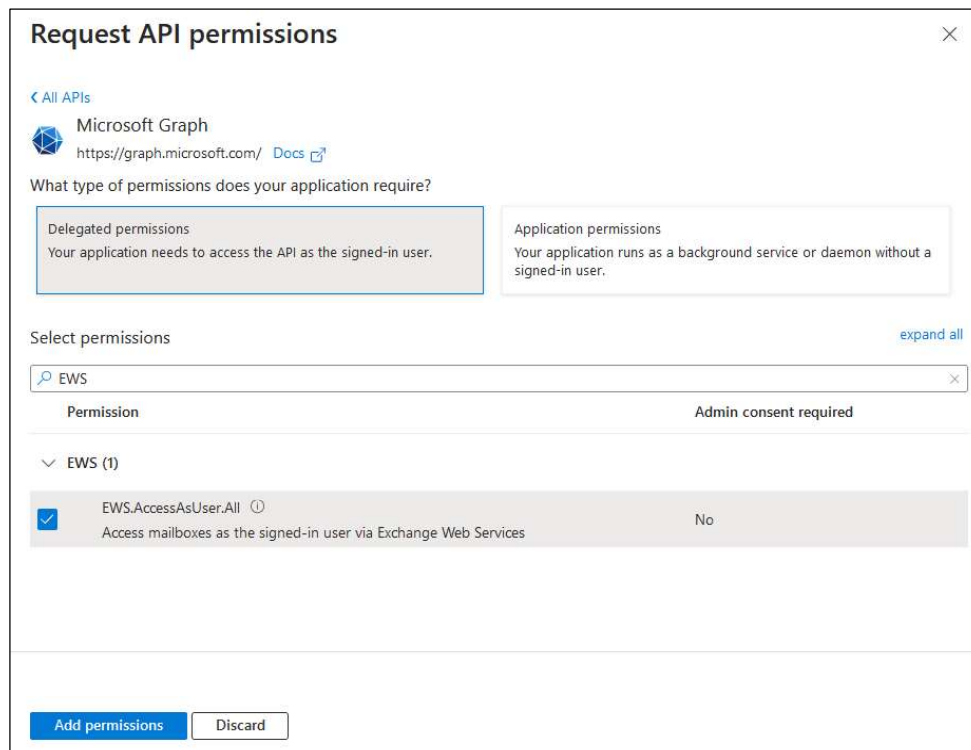
API / Permissions name	Type	Description	Admin consent requi...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...

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

→ 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]**.





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

Home > App registrations > PRM ROPC

PRM ROPC | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators

Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins 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](#)

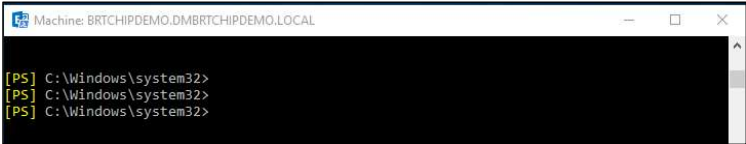

+ Add a permission ✓ Grant admin consent for BRTSYS

API / Permissions name	Type	Description	Admin consent requi...	Status
Microsoft Graph (3)				...
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange Web S...	No	✓ Granted for BRTSYS ...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	✓ Granted for BRTSYS ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for BRTSYS ...

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

## 6. Appendix

### 6.1 Exchange Server setup using Exchange Management Shell – Quick Reference

<p>→ <b>Start Exchange Management PowerShell as an Administrator</b></p>	<p>a. From the exchange server, click <b>Start</b> → <b>Microsoft Exchange Server</b> → <b>Exchange Management Shell</b>. Right-click Exchange Management Shell and select <b>"Run as administrator"</b>.</p> <p>b. The <i>Exchange Management Shell</i> is opened.</p> 
<p>→ <b>Create User Account</b></p>	<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>
<p>→ <b>Create Distribution Group for Users</b></p>	<p>PRM 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>prm-user-group- &lt;groupname&gt;</i>" using the following command –</p> <pre>New-DistributionGroup -Name "prm-user-group- bridgetek1"</pre>
	<p><b>Note:</b> A distribution group name should begin with prefix <i>prm-user-group</i> and be followed by the group name.</p>
	<p>e. Add a user account (<i>user1@bridgetek.com</i>) to an existing user distribution group list (<i>prm-user-group-bridgetek1</i>) using the following command –</p> <pre>Add-DistributionGroupMember -Identity "prm-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 "prm-user-group- bridgetek1"</pre>
<p>→ <b>Create Room / Resource Account</b></p>	<p>g. Using the following command, create a resource account –</p> <pre>New-Mailbox -Name "Room1" -DisplayName "Room1" -Room</pre>
<p>→ <b>Create Distribution Group for Rooms</b></p>	<p>PRM requires rooms to be identified by distribution groups (for example, room1@bridgetek.com). When creating User Groups, omit the <i>RoomList</i> parameter as it is not required.</p>



	<p>h. Create a new room distribution group named "<i>prm-room-group-&lt;groupname&gt;</i>" using the following command -</p> <pre>New-DistributionGroup -Name "prm-room-group-bridgetek1" -RoomList</pre>
	<p><b>Note:</b> A distribution group name should begin with prefix <i>prm-room-group</i> and be followed by the group name.</p>
	<p>i. Add a resource account (<i>room1@bridgetek.com</i>) to an existing room list like (<i>prm-room-group-bridgetek1</i>) using the following command -</p> <pre>Add-DistributionGroupMember -Identity "prm-room-group-bridgetek1" -Member room1@bridgetek.com</pre> <p>j. Use the following command to display a list of rooms that have been added to a particular distribution group -</p> <pre>Get-DistributionGroupMember -Identity " prm-room-group-bridgetek1"</pre>
→ <b>Create Impersonation User / Service Account</b>	<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>
→ <b>Grant Service Account Impersonation Rights – For All (Default)</b>	<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>
→ <b>Grant Service Account Impersonation Rights - For Specific Group (MGMT SCOPE)</b>	<p><b>Create a Distribution Group</b></p> <p>n. Using the following command, create a distribution group to be managed by the impersonation service account -</p> <pre>New-DistributionGroup -Name Bridgetek_Distribution_Group -MemberJoinRestriction open</pre> <p>o. Using the following command, set the distribution group -</p> <pre>Set-DistributionGroup -Identity Bridgetek_Distribution_Group -ManagedBy service-account@bridgetek.com</pre> <p>p. Individual users and rooms may now be added, one by one, into the distribution group, using the following commands:</p>

```
Add-DistributionGroupMember -Identity
Bridgetek_Distribution_Group -Member service-
account@bridgetek.com
```

```
Add-DistributionGroupMember -Identity
Bridgetek_Distribution_Group -Member
user1@bridgetek.com
```

```
Add-DistributionGroupMember -Identity
Bridgetek_Distribution_Group -Member
room1@bridgetek.com
```

```
Get-DistributionGroupMember -Identity
Bridgetek_Distribution_Group
```

For adding bulk accounts / mailboxes, use the following command -

```
Update-DistributionGroupMember -Identity
Bridgetek_Distribution_Group -Members
service-
account@bridgetek.com, user1@bridgetek.com, room1@bri
dgetek.com
```

### **Create Management Scope**

q. Using the following commands, create a management scope -

```
Get-DistributionGroup -Identity
Bridgetek_Distribution_Group | FL name, dist*
```

```
New-ManagementScope -Name
Bridgetek_Management_Scope -
RecipientRestrictionFilter {MemberofGroup -eq
"CN=Bridgetek_Distribution_Group, CN=Users,
DC=DMBRTCHIPDEMO, DC=LOCAL"}
```

```
Get-ManagementScope -Identity
Bridgetek_Management_Scope
```



**Note:** Please provide the DistinguishedName of the distribution group.


### **Create an Impersonation Role Group**


r. Using the following commands, create an Impersonation Role Group -

```
New-RoleGroup -Name
"Bridgetek_Impersonation_Role_Group" -Roles
"ApplicationImpersonation" -
CustomRecipientWriteScope
Bridgetek_Management_Scope -Members service-
account@bridgetek.com
```

```
Get-RoleGroup -Identity
Bridgetek_Impersonation_Role_Group
```

## 6.2 Microsoft 365 setup using Windows PowerShell – Quick Reference

<p>→ <b>Open Windows PowerShell as an Administrator</b></p>	<p>a. Enter PowerShell in Search box, then right-click on the Windows PowerShell icon and select <b>"Run as administrator"</b>.</p> <p>b. In the console, use the following command to install Exchange Online Management Module.</p> <pre>\$Install-Module-Name ExchangeOnlineManagement</pre> <p>c. Using the following command, import the Exchange Online Management Module –</p> <pre>\$ Import-Module ExchangeOnlineManagement</pre> <p>d. Using the following command connect to the Exchange Online Management Module.</p> <pre>Connect-ExchangeOnline -UserPrincipalName Administrator@bridgetek.com</pre> <p>Now the Microsoft 365 can be managed via PowerShell.</p>
<p>→ <b>Create User Account</b></p>	<p>e. 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>
<p>→ <b>Create Distribution Group for Users</b></p>	<p>PRM 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>e. Create a new user distribution group named "<i>prm-user-group- &lt;groupname&gt;</i>" using the following command –</p> <pre>New-DistributionGroup -Name "prm-user-group-bridgetek1"</pre>
	<p><b>Note:</b> A distribution group name should begin with prefix <i>prm-user-group</i> and be followed by the group name.</p>
	<p>f. Add a user account (<i>user1@bridgetek.com</i>) to an existing user distribution group list (<i>prm-user-group-bridgetek1</i>) using the following command –</p> <pre>Add-DistributionGroupMember -Identity "prm-user-group-bridgetek1" -Member user1@bridgetek.com</pre> <p>g. Use the following command to display a list of users who have been added to a particular distribution group –</p> <pre>Get-DistributionGroupMember -Identity "prm-user-group-bridgetek1"</pre>
<p>→ <b>Create Room / Resource Account</b></p>	<p>h. Using the following command, create a resource account –</p>

	<pre>New-Mailbox -Name "Room1" -DisplayName "Room1" -Room</pre>
→ <b>Create Distribution Group for Rooms</b>	<p>PRM requires rooms to be identified by distribution groups (for example, <i>room1@bridgetek.com</i>). When creating User Groups, omit the <i>RoomList</i> parameter as it is not required.</p> <p>i. Create a new room distribution group named "<i>prm-room-group-&lt;groupname&gt;</i>" using the following command -</p> <pre>New-DistributionGroup -Name "prm-room-group-bridgetek1" -RoomList</pre>
	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. A distribution group name should begin with prefix <i>prm-room-group</i> and be followed by the group name.</li> <li>2. Ensure Microsoft 365 groups are not utilized for creating distribution groups</li> </ol>
	<p>j. Add a resource account (<i>room1@bridgetek.com</i>) to an existing room list (<i>prm-room-group-bridgetek1</i>) using the following command -</p> <pre>Add-DistributionGroupMember -Identity "prm-room-group-bridgetek1" -Member room1@bridgetek.com</pre> <p>k. Use the following command to display a list of rooms that have been added to a particular distribution group -</p> <pre>Get-DistributionGroupMember -Identity " prm-room-group-bridgetek1"</pre>
→ <b>Create Impersonation User / Service Account</b>	<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>
→ <b>Grant Service Account Impersonation Rights</b>	<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>

## 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
OIDC	OpenID Connect is an identity authentication protocol that is an extension of open authorization (OAuth) 2.0 to standardize the process for authenticating and authorizing users when they sign in to access digital services.
PRM	The PanL Room Manager is designed to support from large to small organizations to automatically handle meeting room booking issues such as room booking conflicts, ghost bookings, under-utilized rooms, etc.
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

<b>Table 1 – Hardware / Software Requirements .....</b>	<b>4</b>
<b>Table 2 – Network Port Requirements .....</b>	<b>4</b>

## Revision History

Document Title : BRTSYS\_AN\_038 PRM User Guide - 2. Installation and Configuration

Document Reference No. : BRTSYS\_000109

Clearance No. : BRTSYS#070

Product Page : <https://brtsys.com/prm/>

Document Feedback : [Send Feedback](#)

Revision	Changes	Date
Version 1.0	Initial release for PanL Room Manager (PRM) V2.5.0	14-08-2023
Version 2.0	Updated release for PanL Room Manager (PRM) Ver. 3.1.1	04-07-2024