Configuring Office 365 for TPx Managed IDR Service

CUSTOMER GUIDE

CONTENTS

Version 5.0

September 15th, 2022

OVERVIEW

TPx Managed IDR (Inbox and Detection and Response), powered by GoSecure, is an advanced anti-phishing solution, used to submit any suspicious email to the GoSecure Threat Detection Center for expert analysis. The IDR System requires awareness of which users are configured to use the service and must have access to these user mailboxes.

This guide elaborates on required access and how that access can be administered.

PREREQUISITES

- Your Legal Business Name
- Your Business' Physical Address
- Access to the your Microsoft 365 Tenant, through Microsoft Admin Portal for configuring the IDR user Group, Admin Roles, and installing the Outlook add-in for GoSecure IDR.
- At least one Exchange Online (Plan 1) license or higher is required to assign to the Microsoft Global Admin Credentials
- List and count of email users that will be assigned the IDR license within your organization.
- Microsoft Office 365 is required. Microsoft Outlook versions must be fully supported by Microsoft for use with Office 365 (Currently 2016 and newer).
- Expected turn around time to stage and configure GoSecure IDR can vary, based on how long it takes for Microsoft to sync the GoSecure IDR add-in to Outlook.
- To ensure that IDR functions as intended, Exchange Full Access Permissions for the Global Administrator are required for each user mailbox that will be using IDR (a breakdown of the different impersonation and EWS in exchange can be found here).
    - This is specifically to facilitate the IDR application to move reported messages from an individual user inbox to the quarantine folder in Exchange, and to return messages deemed as "Safe" back to the original submitter's inbox.
    - ApplicationImpersonation is also Required for IDR to function as intended.
- Multi-Factor Authentication through Azure Active Directory is supported

MICROSOFT OFFICE 365 AND IDR TENANT CONFIGURATION

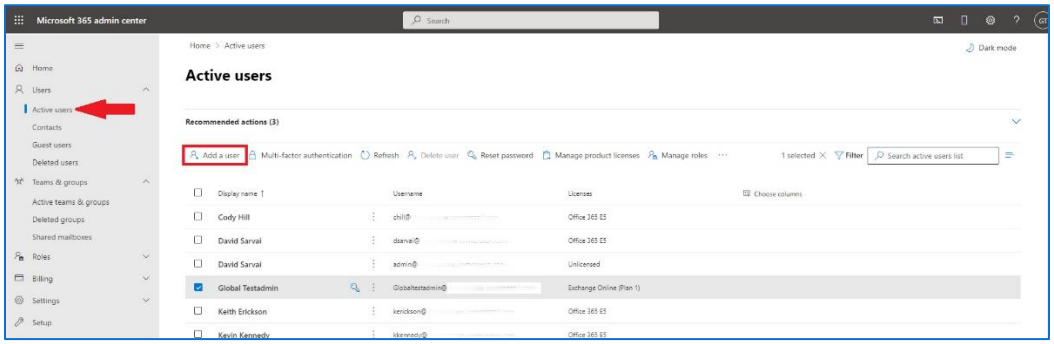
Note that Microsoft 365 tenant configuration and IDR portal configuration is required to enable this service. You are responsible for configuring your Microsoft 365 Tenant, and TPx is responsible for configuring the GoSecure IDR Portal. Your TPx team is available to assist you with Office 365 Configuration if you run into any issues.

STEP 1: CONFIGURE A GLOBAL ADMINISTRATOR USER IN THE MICROSOFT ADMIN CENTER FOR IDR

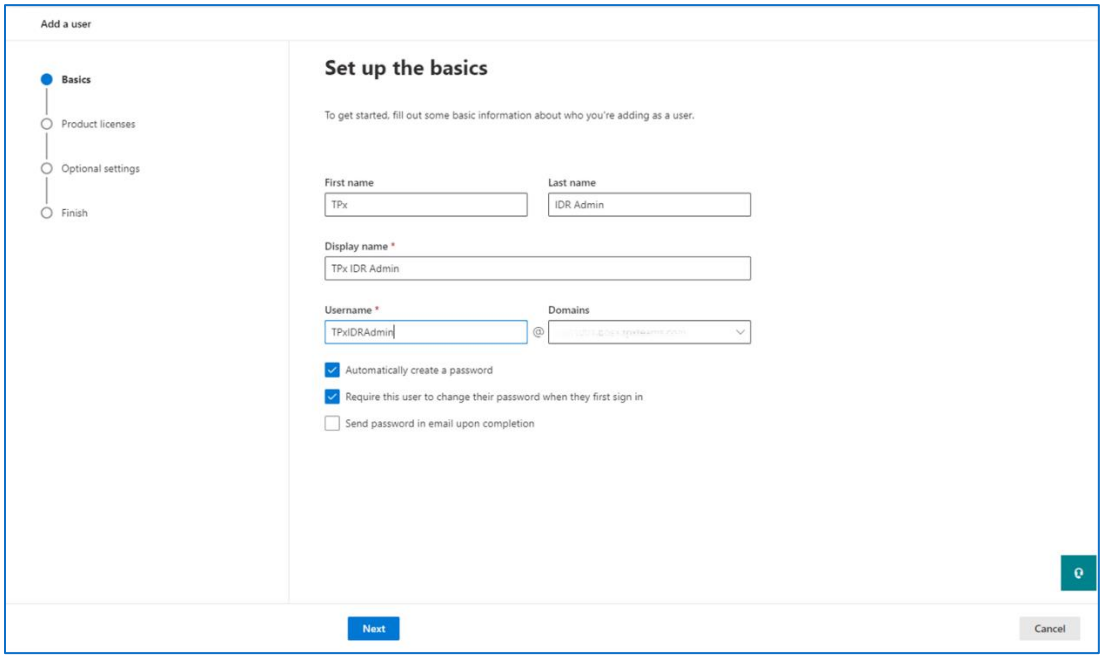
IDR requires a local Tenant Global Admin to function properly. This user is intended only for IDR, not with an actual user in your organization.

NOTE: You must login with a pre-existing Global Admin Account to create another Global Admin.

1. Login to https://admin.microsoft.com/.
2. Click **Users** in the navigation pane and select **Active Users**.
3. On the **Active Users** screen, select **Add a User**.

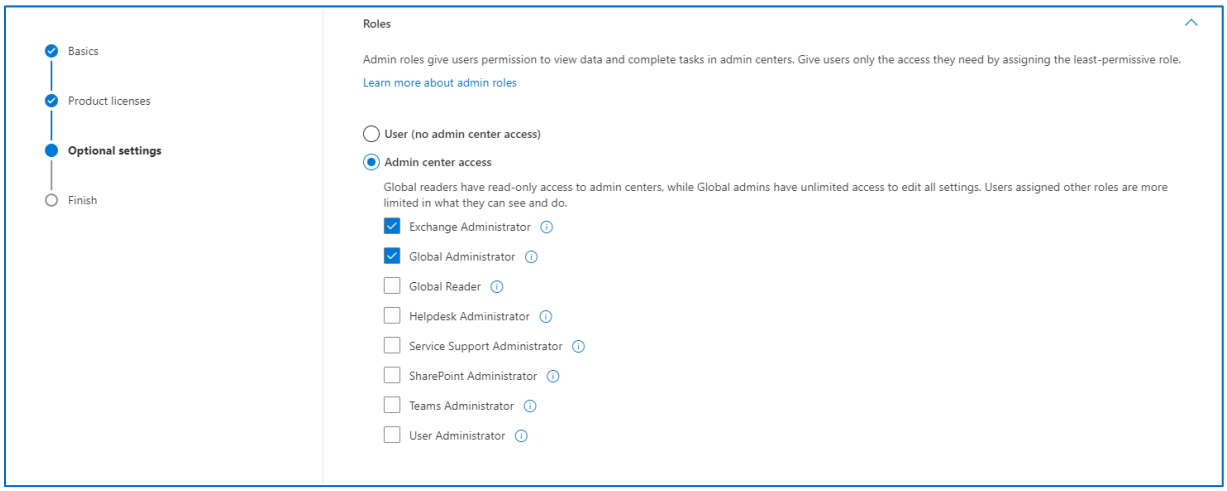


4. Enter **TPx IDR Admin** for the **Display name** and **Username**, then select **Next**.



	**NOTE:** Please keep a record of the full username (and the domain) as well as the password. This information is provided to the TPx team to setup the GoSecure IDR Portal.

5. On the next page, assign an available **Exchange Online (Plan 1)** license, then select **Next**. If you do not have an available Exchange Online Plan 1 license you can use any available Microsoft 365 license that includes Exchange Online Plan 1 or acquire a license through your chosen provider.
6. On the following page, go to **Optional settings** to access the **Roles** section.
7. Select **Admin center access**, then enable the following permissions:



   a. Exchange Administrator
   b. Global Administrator
      i. Application Administrator

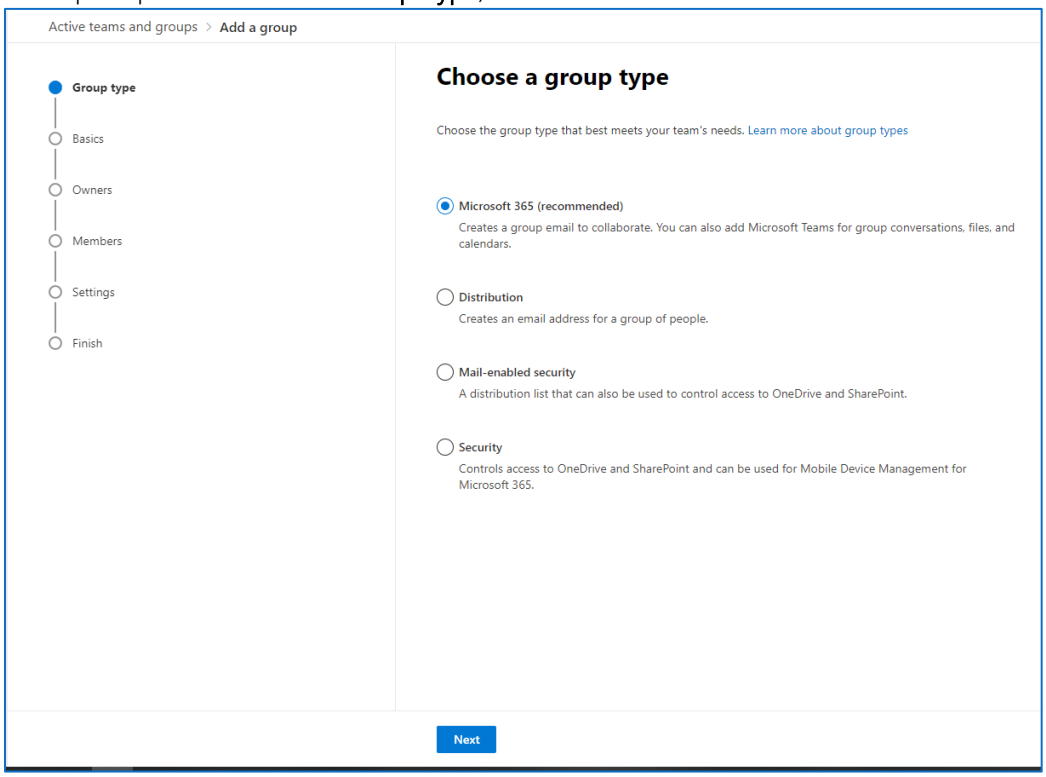
	**NOTE:** You may need to select "Show All by Category" to show this role; it is listed under **Identity**.

8. Click **Save**.

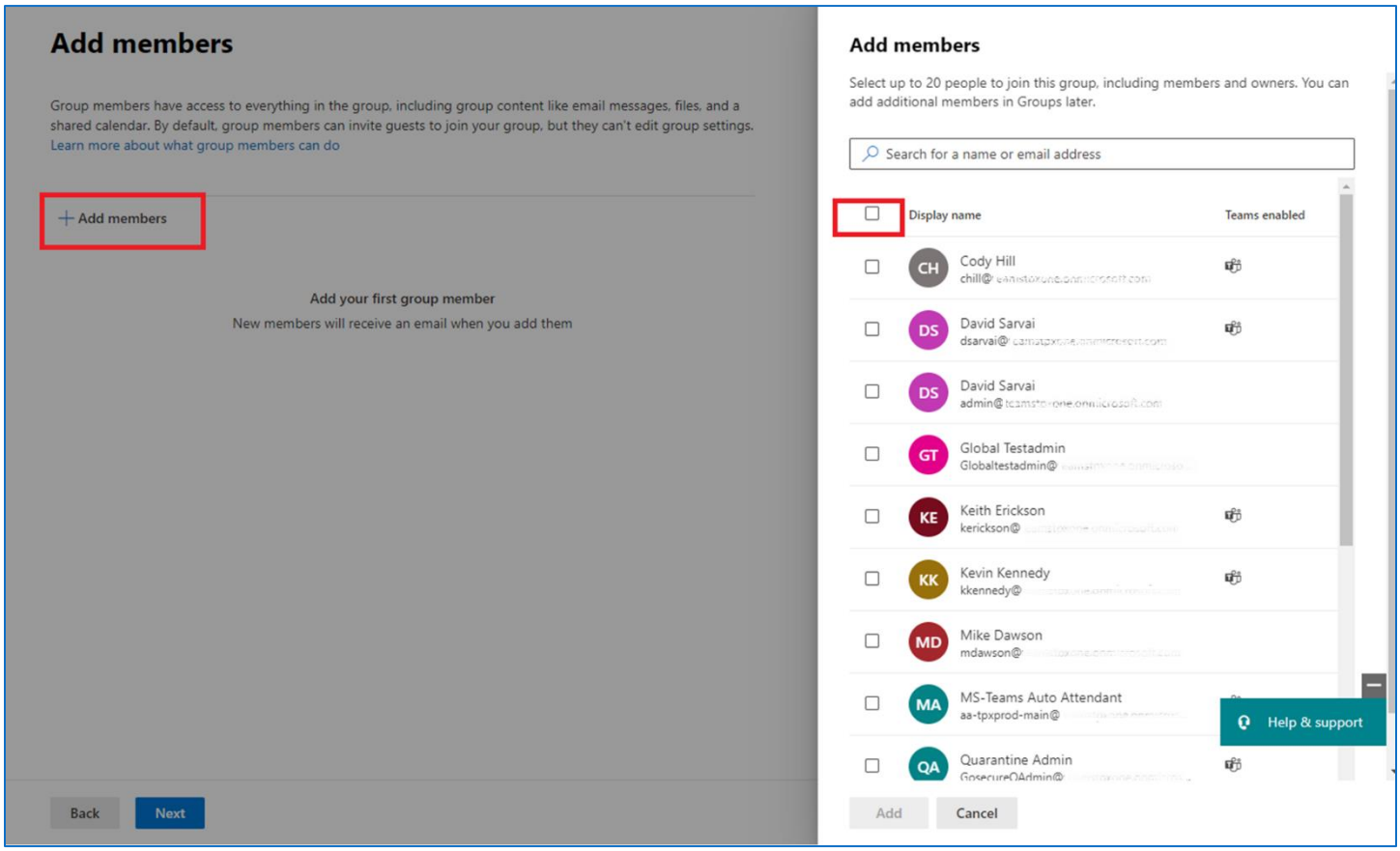
STEP 2: IDENTIFY OR CREATE A GROUP OF USERS IN MICROSOFT ADMIN CENTER FOR IDR

IDR uses an Exchange Group to identify which users should have access to the system. Only users in this group can use the service. This group is used in the IDR Portal as well as when you deploy the Outlook add-in in the Microsoft 365 Admin Center.

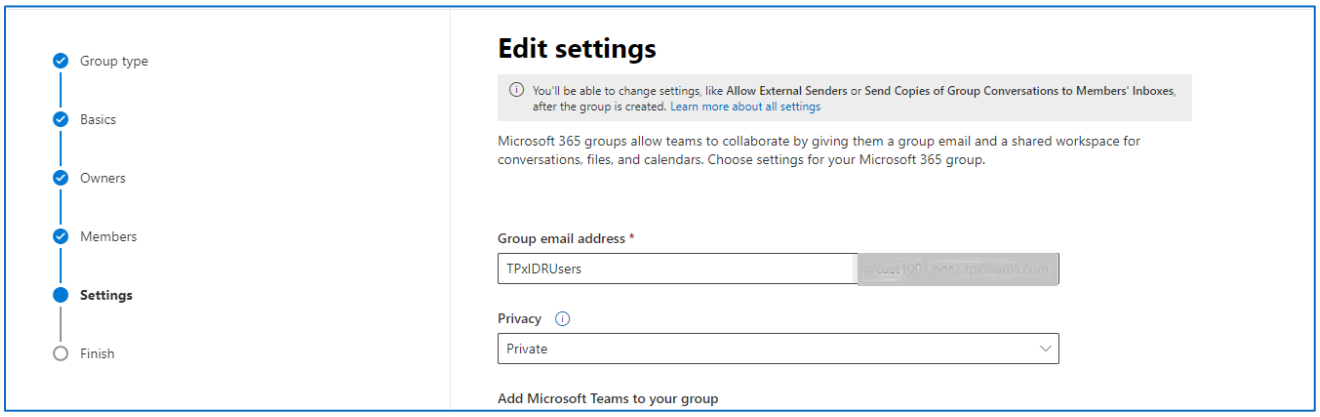
1. Login to Microsoft Admin Center as the **TPx IDR Admin**.
2. In the Navigation Pane, expand the **Teams & Groups** section, and select Active Teams & Groups.
3. Click **Add a Group**.
4. When prompted to **Choose a Group Type**, select **Microsoft 365** and then click **Next**.



5. Enter **TPx IDR Users** for the **Group Name**, then select **Next**.
6. Enter **TPx IDR Admin** for the **Group Owner**, then select **Next**.
7. In the next **Add Members** screen, select **add members**. A new pane displays on the right.

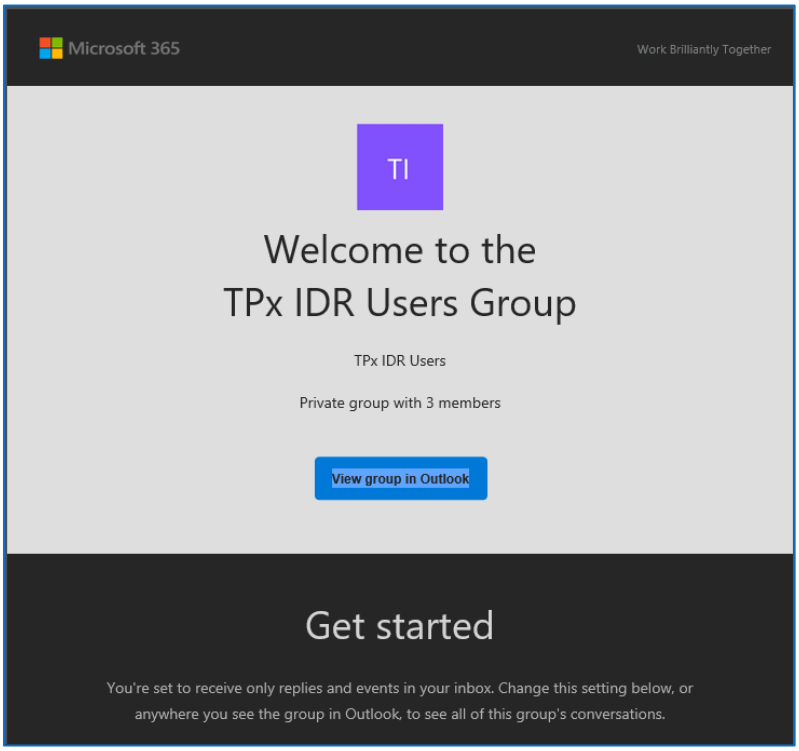


8. Select users to add to this group. To add in bulk, select the checkmark icon in the column header.
9. Click **Next**.
10. In the **Edit settings** screen, enter the group email address as TPxIDRUsers@*(your domain)* and select **Private** from the Privacy drop-down menu. This user is used to search and connect the Microsoft group to the GoSecure IDR Portal.
11. Click **Next**.



12. Review the group settings and confirm all users are listed in the members list for the GoSecure IDR license, then click **Create Group**.

	NOTE: Once the TPx IDR Users Group is created, each user receives an email from Microsoft, notifying them they are now added.

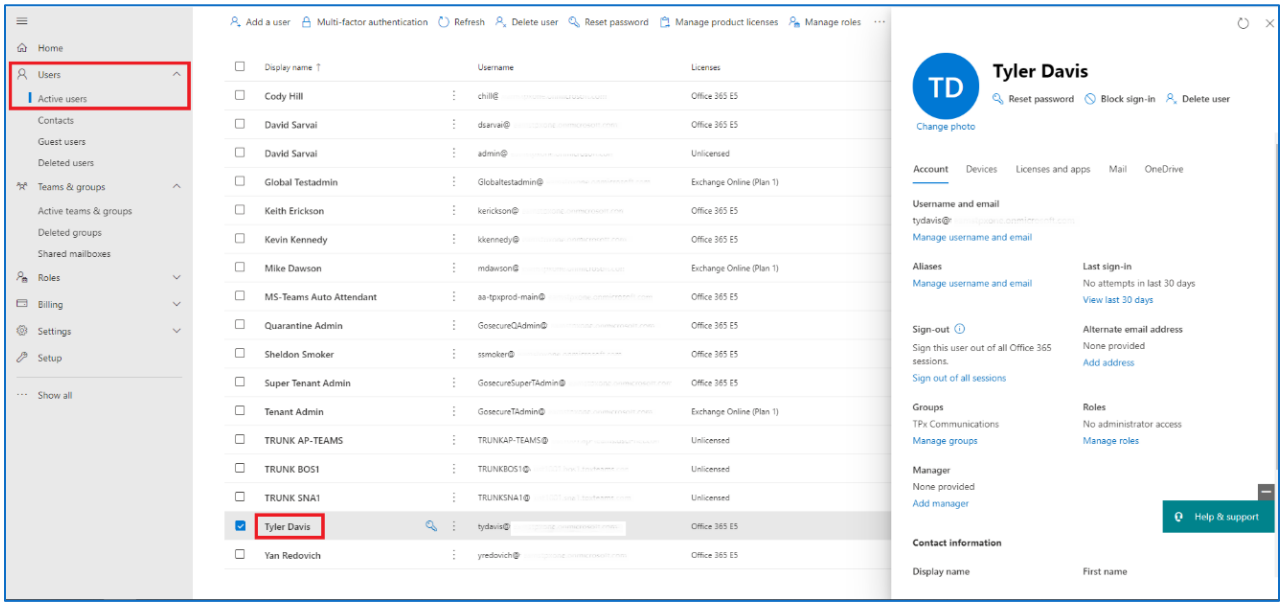


STEP 3: GLOBAL ADMIN MAILBOX FOLDER PERMISSIONS

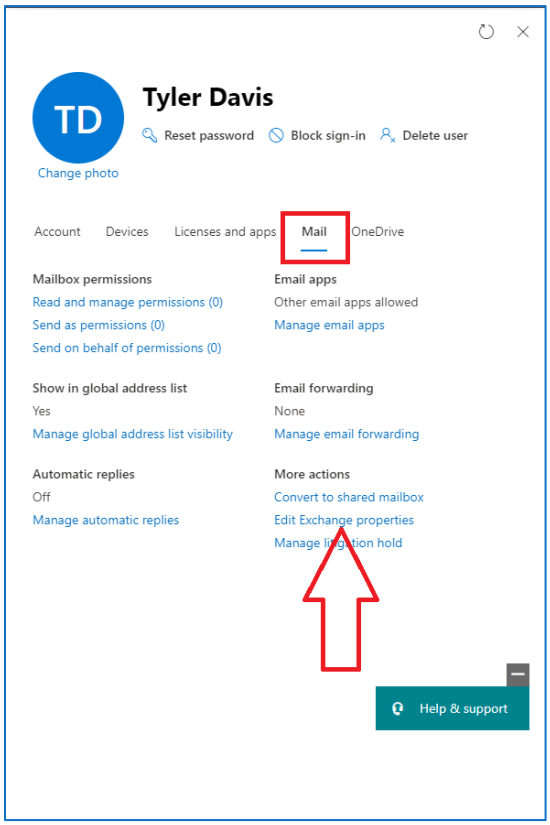
To ensure messages can be properly utilized by the GoSecure IDR application, primarily for messages to be properly removed from a user's inbox and placed into quarantine, as well as returning safe messages. Each user assigned to the "TPx IDR Users" group will need to follow through these steps.

NOTE: If there are several users within the "TPx IDR Users" group, you can reference which users are in the group by navigating to "Teams and Groups" and selecting "Active teams & Groups".

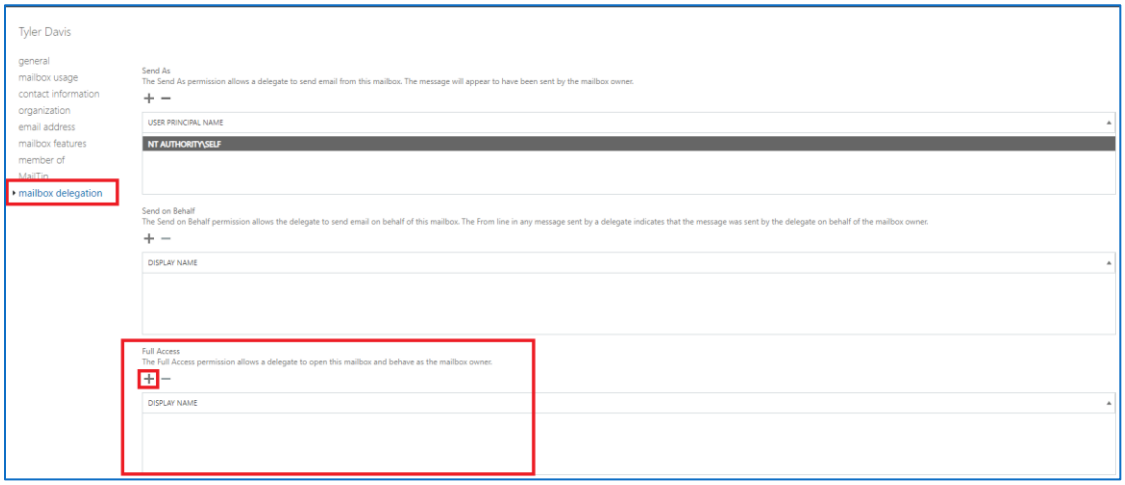
1. From Microsoft Admin Center, navigate to **Users**, then select **Active Users**.
2. Select a user assigned to **TPx IDR Users** in Step 2, then click their Display name.



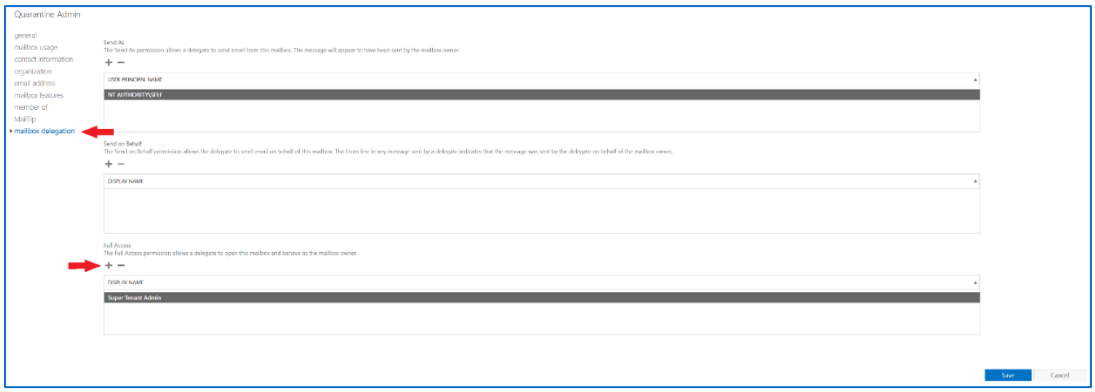
3. On the new window that appears on the right side of your screen, click the **Mail** tab.



4. Select **Edit Exchange properties**.
5. On the navigation pane, select **Mailbox Delegation**.
6. Click the **+** icon in the **Full Access** section.



7. Select our **TPx IDR Admin** from the list, then click **Add**.
8. Click **OK**. This returns to the **Mailbox Delegation** section.
9. Verify the **TPx IDR Admin** now displays.



10. Repeat this process for each user in the **TPx IDR Users** group.

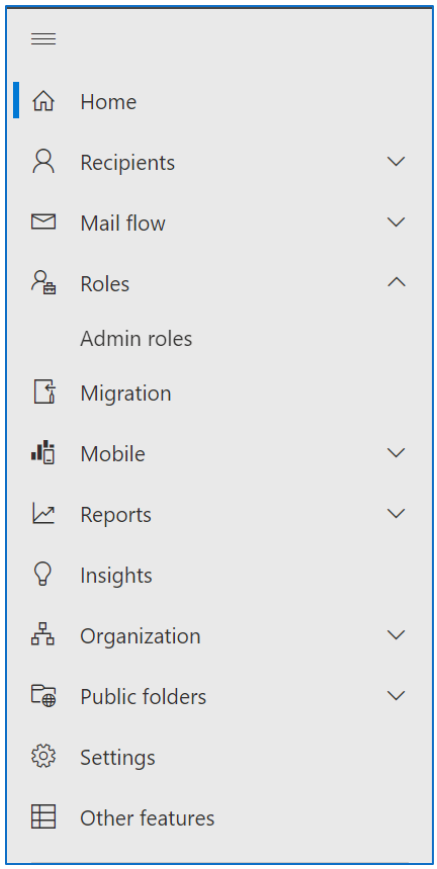
NOTE: Alternatively, use the following PowerShell Script to automate the full access folder permissions. Confirm you are able to connect to Exchange Online through PowerShell, and the correct permissions.

- PowerShell Automation Script:

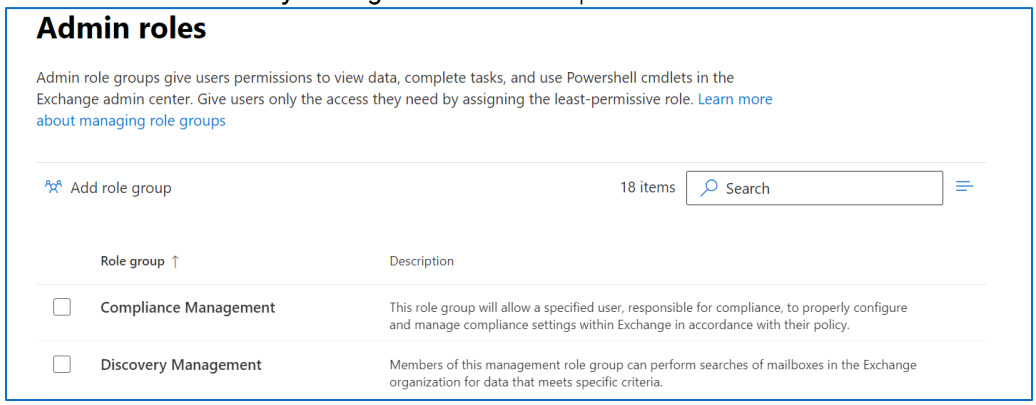
```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox') -and (Alias -ne 'TPx IDR Admin')} | Add-MailboxPermission -User TPxIDRAdmin@gosecure.net -AccessRights fullaccess -InheritanceType all -AutoMapping:$false
```

STEP 5: ADJUST APPLICATION IMPERSONATION PERMISSIONS IN EAC

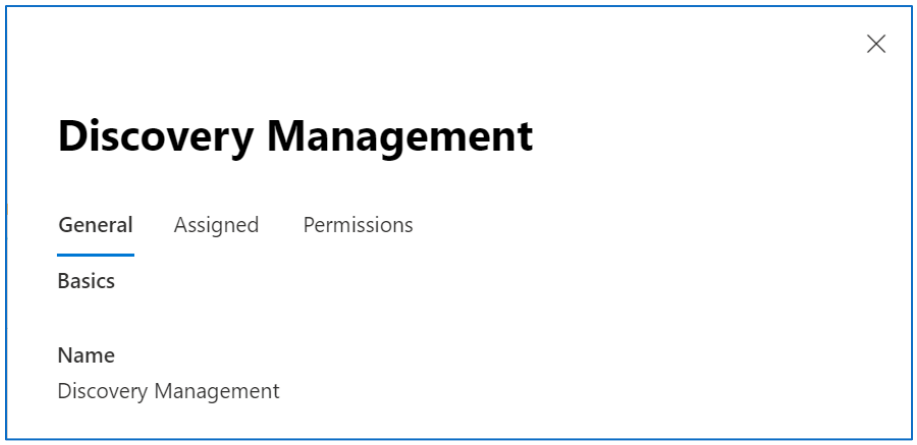
1. Navigate to Exchange Admin Center
2. Locate the **Roles** Section in the navigation Pane and select **Admin Roles**



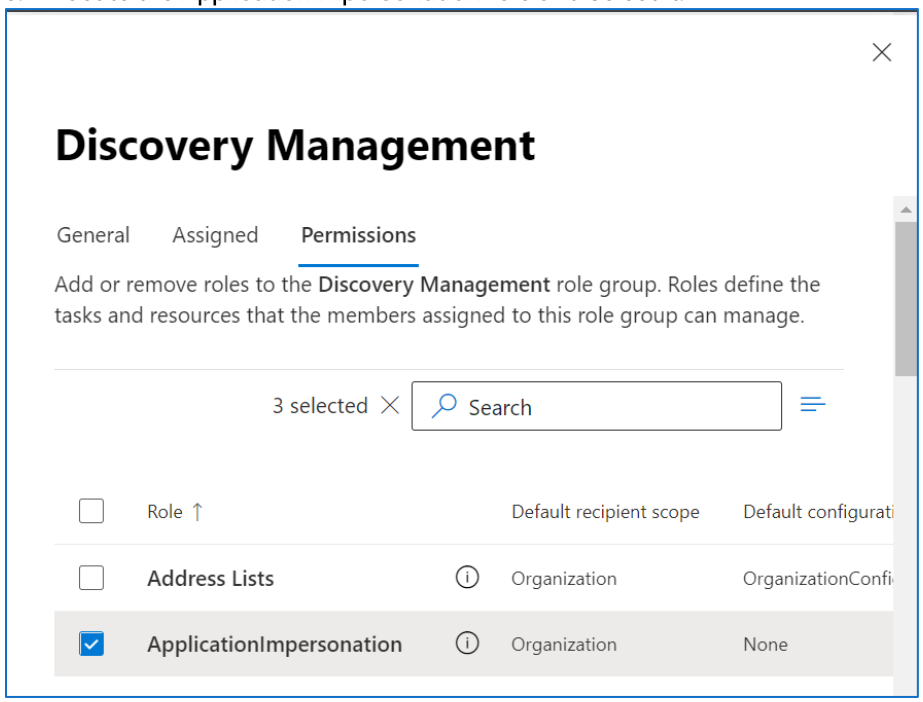
3. Locate the **Discovery Management** Role Group and select it



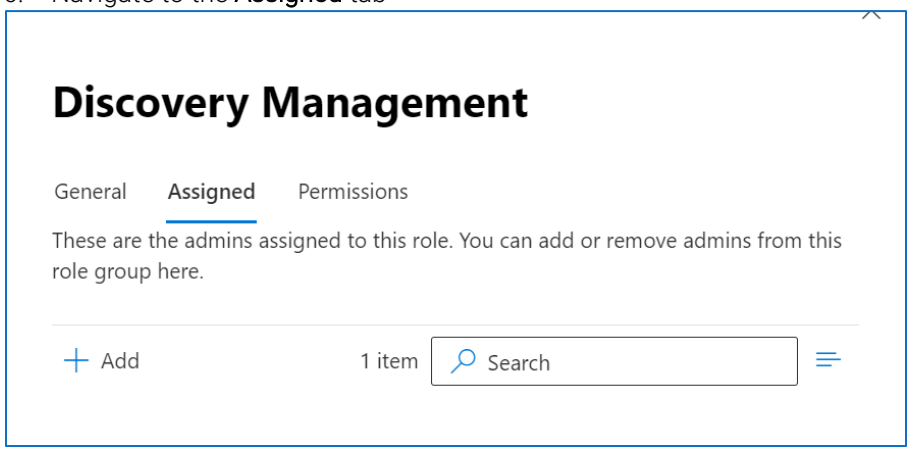
4. In the discovery management Drawer, navigate to the **Permissions** tab



5. Locate the **ApplicationImpersonation** role and select it.



6. Navigate to the **Assigned** tab



7. Select **Add** and enter in the TPx IDR Admin and hit **Add**
8. Select **Save** at the bottom of the drawer.

STEP 6: GRANT THE IDR APPLICATION ACCESS TO THE MAILBOXES

This step assigns one of two permissions needed to allow GoSecure IDR to access the mailboxes in our **TPx IDR Users** group. Please reach out to your TPx representative for assistance setting up and configuring the GoSecure IDR Portal.

NOTE: You need to provide TPx with the **TPx IDR Admin** credentials from Step 1.

STEP 7: CONFIGURE IDR TO PROVISION THE GROUP OF USERS

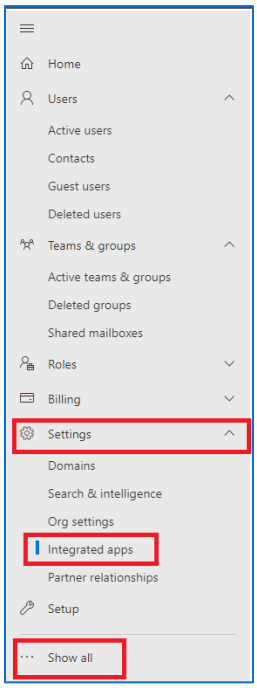
This step associates the Mailbox group you created in Step 2, within the GoSecure IDR Admin Portal. Please reach out to your TPx representative for assistance setting up and configuring the GoSecure IDR Portal.

NOTE: For the next step, TPx needs to provide you with the **Add-in URL** included in the GoSecure IDR Admin Portal.

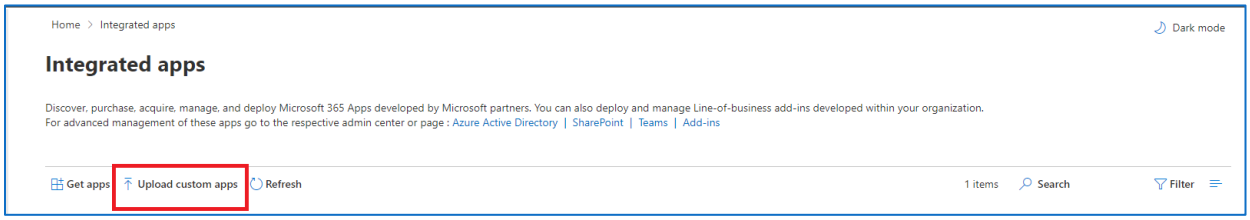
STEP 8: INSTALL THE OUTLOOK ADD-IN IN THE MICROSOFT 365 ADMIN CENTER

Before starting, confirm you have the **Add-in URL** from TPx. This step is necessary to display the GoSecure IDR Add-in for users within their Outlook clients.

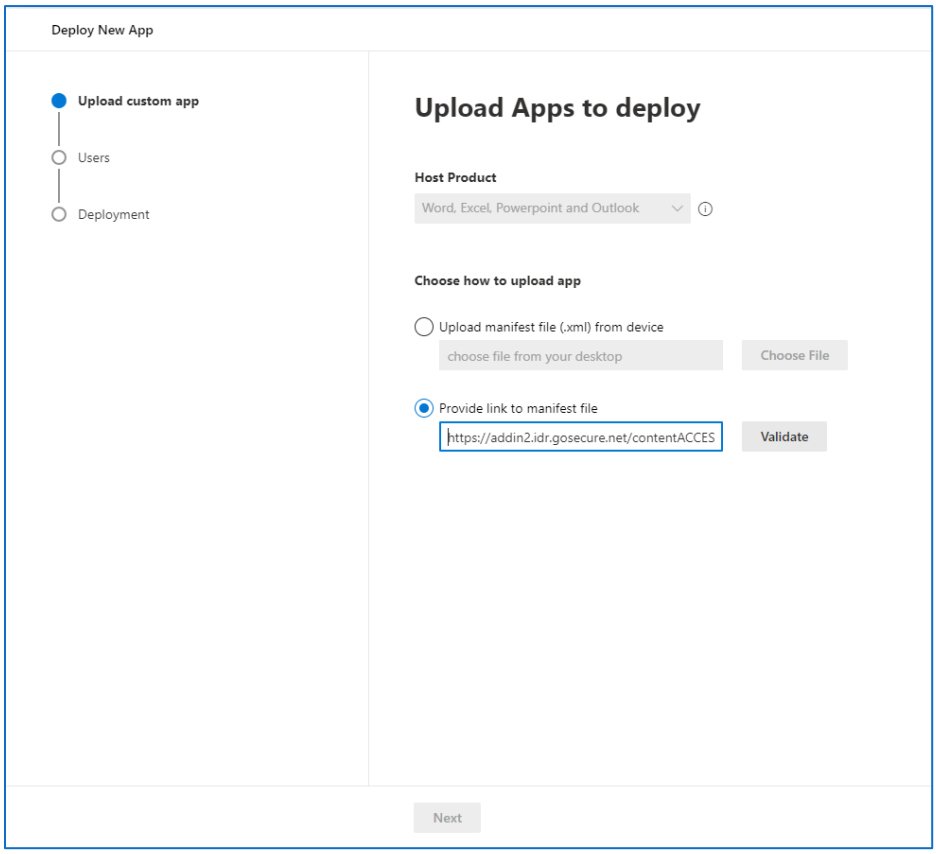
1. Login to Microsoft Admin Center, using the **TPx IDR Admin** credentials created in Step 1.
2. In the navigation pane, select **Show All** and locate the **Settings** section.
3. Select **Integrated Apps**.



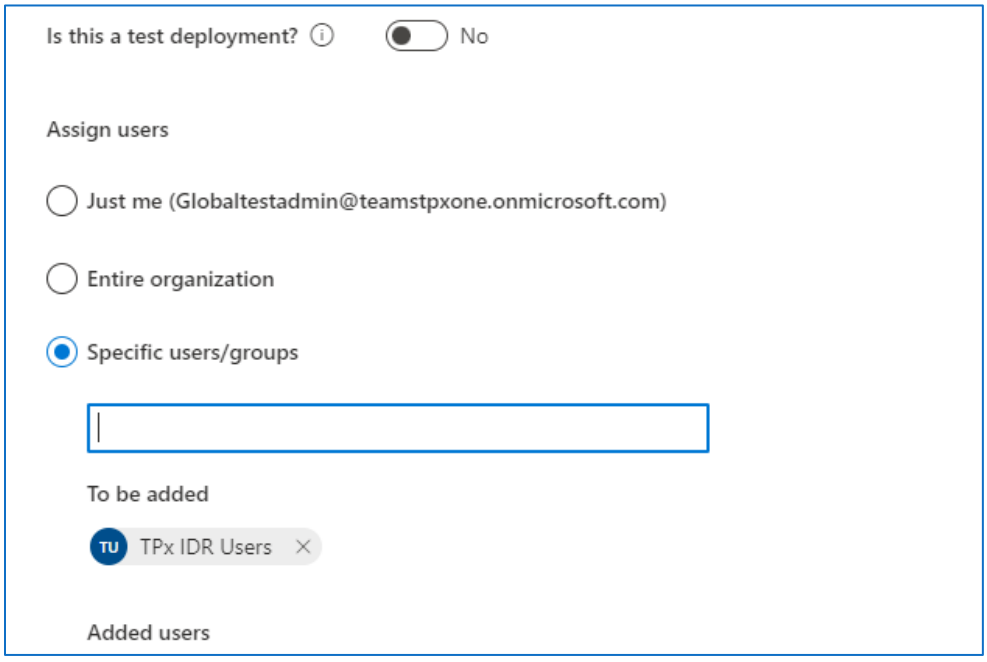
4. Select **Upload Custom App**.



5. Under **Upload Apps to deploy**, select **Provide link to manifest file** and paste the URL you received from Step 5.
6. Click **Validate**, then click **Next**.



7. Select Specific users/groups and enter the group name TPx IDR Users.



8. Select Next to accept the permissions request to deploy the app.
9. Confirm the deployment on the next page.

NOTE: Typically, the Outlook add-in displays within 15 minutes or so. However, there are a few situations where the Outlook Add-in may not be visible in the user's mailbox for several hours. This is a Microsoft limitation and expected behavior with office add-ins.

STEP 9: GOSECURE IDR ADMIN CENTER AND ACCOUNT CONFIGURATION

After associating the GoSecure IDR add-in for Outlook, contact your TPx representative to grant you access to the GoSecure IDR Admin Portal and to finish the configuration of your GoSecure IDR Account.

STEP 10: VALIDATE THE INSTALLATION

If you encounter any challenges throughout this onboarding process, the following application areas can be accessed to validate the proper permissions and access were configured:

NOTE: Please work with your TPx representative to address any validation concerns with the installation and onboarding of GoSecure IDR.

MICROSOFT ADMIN PORTAL

- The Customer Admin Portal for Microsoft 365 has a new section available (Integrated Apps) within the navigation pane if GoSecure successfully synched with the Exchange Mailbox Group we setup in Step 2 and the add in deployment in Step 6. This may take several hours before Microsoft picks up IDR to display in this section.

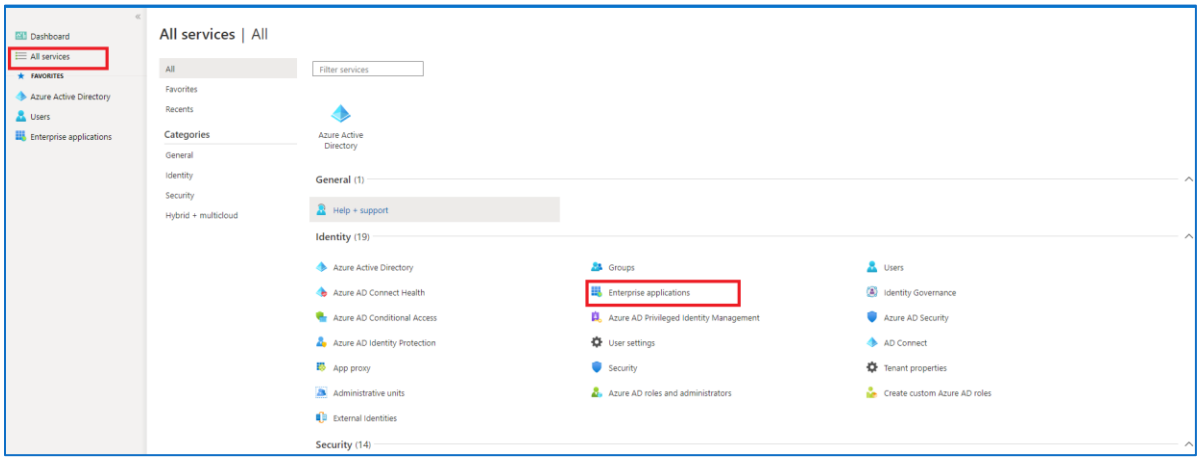
OUTLOOK

- Confirm that the Outlook plugin for GoSecure IDR displays within the outlook ribbon (desktop client) or is nested in the ellipsis Icon (Outlook Web). If the button does not display within outlook, review Step 6 to ensure that the enterprise app was configured properly.
- If the button does display, however the end user is prompted to "Login" to the plugin, verify within Microsoft Admin Center that the "IDR Global Admin" has "Full Access" to the "TPx IDR Users Group" under "Mailbox Delegation" in Step 3.
- The other necessary permission, GoSecure IDR Prod Azure Admin, can be found within the Azure Admin Center. This allows for the IDR Global Admin's login credentials to persist access to the GoSecure IDR Add in.

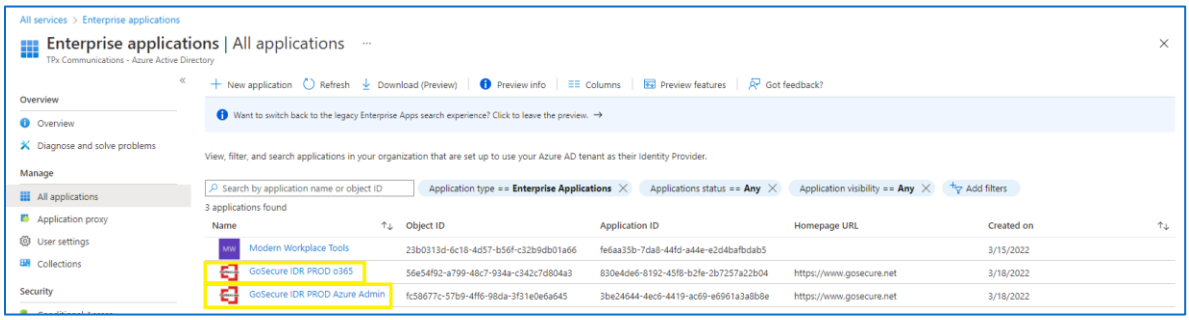
NOTE: End users cannot log into this section with their own login credentials.

AZURE ADMIN CENTER

- This confirms the Microsoft Global Administrator accepted the proper permissions for GoSecure to have perpetual access to the Exchange server (this facilitates the action on messages within exchange, directly from GoSecure IDR).
- There are two applications to verify in the "Enterprise Applications" section in Azure Admin Center. Select **All Services** in the left navigation pane then click **Enterprise Applications** under the "Identity" Category.



  - From the **Enterprise Applications** section, the following applications display:



  - GoSecure IDR PROD o365
    - These permissions display when TPx initially logs the global administrator into the GoSecure Portal in Step 4.
  - GoSecure IDR Prod Azure Admin
    - These permissions display when TPx initially configures the GoSecure IDR Admin Portal.