

# Configuring Office 365 for TPx Managed IDR Service







### CONTENTS

Overview	3
Prerequisites	
Microsoft Office 365 and IDR Tenant Configuration	
Step 1: Configure a Global Administrator User in the Microsoft Admin Center for IDR	
Step 2: Identify or Create a Group of Users in Microsoft Admin Center for IDR	7
Step 5: Adjust Application Impersonation Permissions in EAC	
Step 6: Grant the IDR Application Access to the Mailboxes	15
Step 7: Configure IDR to Provision the Group of Users	15
Step 8: Install the Outlook Add-In in the Microsoft 365 Admin Center	15
Step 9: GoSecure IDR Admin Center and Account Configuration	
Step 10: Validate the Installation	18
Microsoft Admin Portal	
Outlook	
Azure Admin Center	19

Version 5.0 September 15<sup>th</sup>, 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 <u>here</u>).
  - 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.

::: Microsoft 365 admin center		,O Search			0 <b>e</b> ? (e
=	Home > Active users				👌 Dark mode
ώ Home	Active users				
R Users /					
Active users	Recommended actions (3)				~
Guest users Deleted users	Add a user	ish 🔍 Delete user 🔍 Reset password 📋 M	Janage product licenses $  \beta_{\mathbf{b}} $ Manage roles $ \cdots $	1 selected $\times$ $\nabla$ Filter $\bigcirc$ Search active users in	я <b>—</b>
ጎድ Teams & groups / Active teams & groups	Display name †	Usemanie	Licenses	E Choose columns	
Deleted groups	Cody Hill	chill®	Office 165 E5		
Shared mailboxes	David Sarvai	dsarvai@	Office 365 E5		
Pin Roles	David Sarval	admin@	Unlicersed		
E Billing	Global Testadmin 🔍 :	Globaltestadmin@	Eschange Online (Flan 1)		
Settings	Keith Erickson	kerickson@	Office 365 E5		
S. amah	Kevin Kennedy	kkenned/@	Office 265 65		

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

Add a user		
Basics	Set up the basics	
Product licenses	To get started, fill out some basic information about who you're adding as a user.	
Optional settings	First name Last name	
O Finish	TPx IDR Admin	
	Display name *	
	TPx IDR Admin	
	Username * Domains	
	TPxIDRAdmin	
	Automatically create a password	
	Require this user to change their password when they first sign in	
	Send password in email upon completion	
	Next	Cance





**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:

	Roles	^
Basics	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 rol	e.
Product licenses	Learn more about admin roles	
Froduct licenses		
Optional settings	User (no admin center access)	
	Admin center access	
) Finish	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 Administrator 🕕	
	Global Administrator 🕕	
	Global Reader 🛈	
	Helpdesk Administrator 🛈	
	Service Support Administrator ()	
	SharePoint Administrator 🕕	
	Teams Administrator ()	
	User Administrator 🛈	

- 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**.



Identity         Application Administrator ①         Application Developer ①         Authentication Administrator ①         Cloud Application Administrator ①         Conditional Access Administrator ①         Domain Name Administrator ①         External Identity Provider Administrator ①         Guest Inviter ①         Helpdesk Administrator ①         Hybrid Identity Administrator ①         License Administrator ①		
<ul> <li>Application Administrator ①</li> <li>Application Developer ①</li> <li>Authentication Administrator ①</li> <li>Cloud Application Administrator ①</li> <li>Conditional Access Administrator ①</li> <li>Domain Name Administrator ①</li> <li>External Identity Provider Administrator ①</li> <li>Guest Inviter ①</li> <li>Helpdesk Administrator ①</li> <li>License Administrator ①</li> </ul>	lde	entity
Application Developer   Authentication Administrator   Cloud Application Administrator   Conditional Access Administrator   Domain Name Administrator   Domain Name Administrator   External Identity Provider Administrator   Guest Inviter   Helpdesk Administrator   Hybrid Identity Administrator   License Administrator	~	Application Administrator 🕕
Authentication Administrator  Cloud Application Administrator  Conditional Access Administrator  Domain Name Administrator  External Identity Provider Administrator  External Identity Provider Administrator  Helpdesk Administrator  License Administrator  U		Application Developer 🕜
<ul> <li>Cloud Application Administrator ①</li> <li>Conditional Access Administrator ①</li> <li>Domain Name Administrator ①</li> <li>External Identity Provider Administrator ①</li> <li>Guest Inviter ①</li> <li>Helpdesk Administrator ①</li> <li>Hybrid Identity Administrator ①</li> <li>License Administrator ①</li> </ul>		Authentication Administrator ()
<ul> <li>Conditional Access Administrator ①</li> <li>Domain Name Administrator ①</li> <li>External Identity Provider Administrator ①</li> <li>Guest Inviter ①</li> <li>Helpdesk Administrator ①</li> <li>Hybrid Identity Administrator ①</li> <li>License Administrator ①</li> </ul>		Cloud Application Administrator 🕦
<ul> <li>Domain Name Administrator ①</li> <li>External Identity Provider Administrator ①</li> <li>Guest Inviter ①</li> <li>Helpdesk Administrator ①</li> <li>Hybrid Identity Administrator ①</li> <li>License Administrator ①</li> </ul>		Conditional Access Administrator ()
<ul> <li>External Identity Provider Administrator ()</li> <li>Guest Inviter ()</li> <li>Helpdesk Administrator ()</li> <li>Hybrid Identity Administrator ()</li> <li>License Administrator ()</li> </ul>		Domain Name Administrator ()
Guest Inviter ① Helpdesk Administrator ① Hybrid Identity Administrator ① License Administrator ①		External Identity Provider Administrator ()
Helpdesk Administrator ①         Hybrid Identity Administrator ①         License Administrator ①		Guest Inviter ()
Hybrid Identity Administrator ①         License Administrator ①		Helpdesk Administrator 🕕
License Administrator 1		Hybrid Identity Administrator ()
		License Administrator 🕦

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.

Group type	Choose a group type
Basics	Choose the group type that best meets your team's needs. Learn more about group types
) Owners	Microsoft 365 (recommended)
) Members	Creates a group email to collaborate. You can also add Microsoft Teams for group conversations, files, a calendars.
) Settings	Olistribution
) Finish	Creates an email address for a group of people.
	O 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.

- 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.



Add members	Add members				
Group members have access to everything in the group, including group content like email messages, files, and a shared calendar. By default, group members can invite guests to join your group, but they can't edit group settings.	Select up to 20 people to join this group, including members and owners. You car add additional members in Groups later.				
Learn more about what group members can do	$\wp$ Search for a name or email address				
+ Add members	Display name	Teams enabled			
	CH Cody Hill chill@rearistoxune.com/costit.com	லீற்			
New members will receive an email when you add them	David Sarvai dsarvai@castazaxaa.commerceson.com	<b>u</b> <sup>2</sup> β			
	David Sarvai admin@ teamstorome.connilcrosoft.com				
	Global Testadmin Globaltestadmin@ counsines come.coso				
	Keith Erickson kerickson	16 <sup>°</sup> D			
	KK Kevin Kennedy kkennedy@	ifj:			
	Mike Dawson mdawson@				
	MS-Teams Auto Attendant aa-tpxprod-main@	e Help & support			
	Quarantine Admin Gosecure OAdmin@	ម្រី			
Back Next	Add Cancel				

- 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.

✓ Group type	Edit settings	
Rasics	You'll be able to change settings, like Allow Extern after the group is created. Learn more about all se	nal Senders or Send Copies of Group Conversations to Members' Inboxes, ettings
Owners	Microsoft 365 groups allow teams to collaborate conversations, files, and calendars. Choose settin	by giving them a group email and a shared workspace for gs for your Microsoft 365 group.
<ul> <li>Members</li> </ul>	Group email address *	
	TPxIDRUsers	w.cust1001.bos1.tpxteams.com
Settings		
	Privacy ()	
, Finish	Private	$\sim$

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 <u>Step 2</u>, then click their Display name.

=		🔍 Add a user 🛛 🔒 Multi-factor authentica	tion 💍 Re	fresh 🔗 Delete user 🔍 Reset password 📋 N	Vlanage product licenses 🦂 Manage roles \cdots		ů ×
없 Home 옷 Users	~	□ Display name ↑		Usemame	Licenses	Tyler Day	vis
Active users		Cody Hill		chill@	Office 365 E5	Reset passwork	d 🚫 Block sign-in 🔒 Delete user
Contacts		David Sarvai	:	dsarvai@	Office 365 E5	Change photo	
Guest users		David Sarvai	:	admin@	Unlicensed		
ሻጽ Teams & groups	~	Global Testadmin	:	Globaltestadmin@	Exchange Online (Plan 1)	Account Devices Licenses and	apps Mail OneDrive
Active teams & groups		Keith Erickson		kerickson@ commonsorm row	Office 365 E5	Username and email	
Deleted groups		C Kevin Kennedy		kkennedy@ months on microcott com	Office 365 E5	Manage username and email	
Shared mailboxes	~	Mike Dawson	:	mdawson@	Exchange Online (Plan 1)	Aliases	Last sign-in
Billing	~	MS-Teams Auto Attendant		aa-tpxprod-main@	Office 365 E5	Manage username and email	No attempts in last 30 days View last 30 days
Settings	~	Quarantine Admin		GosecureQAdmin@	Office 365 E5	Sign-out 🕕	Alternate email address
		Sheldon Smoker	:	ssmoker@	Office 365 E5	Sign this user out of all Office 365 sessions.	None provided Add address
		Super Tenant Admin	:	GosecureSuperTAdmin@	Office 365 E5	Sign out of all sessions	
Snow all		Tenant Admin	:	GosecureTAdmin@	Exchange Online (Plan 1)	Groups	Roles
		TRUNK AP-TEAMS	:	TRUNKAP-TEAMS@	Unlicensed	Manage groups	Manage roles
		TRUNK BOS1	:	TRUNKBOS1@ 0010001 hos 1 textes ere con	Unlicensed	Manager	
		TRUNK SNA1		TRUNKSNAT@ cot1001 seal texteses com	Unlicensed	None provided Add manager	
		Tyler Davis	۹ :	tydavis@	Office 365 E5	-	P Help & support
		Yan Redovich		yredovich@	Office 365 E5	Contact information	
						Display name	First name

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



Change photo	d ∣ O Block sign-in ⊢X, Delete user
change photo	
Account Devices Licenses and	apps Mail OneDrive
Mailbox permissions	Email apps
Read and manage permissions (0)	Other email apps allowed
Send as permissions (0)	Manage email apps
Send on behalf of permissions (0)	
Show in global address list	Email forwarding
Yes	None
Manage global address list visibility	Manage email forwarding
Automatic replies	More actions
Off	Convert to shared mailbox
Manage automatic replies	Edit Exchange properties
	Manage lingution hold
	<u> </u>

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

Tyler Davis		
general mailbox usage contact information organization email address	Send As The Send As permission allows a delegate to send email from this mailbox. The message will appear to have been sent by the mailbox owner. +	*
mailbox features member of MailTin • mailbox delegation	NT AUTHORITYSEUS	
- Hundek delegation	Send on Behalf The Send on Behalf permission allows the delegate to send email on behalf of this mailbox. The From line in any message sent by a delegate indicates that the message was sent by the delegate on behalf of the mailbox ownes. + -	
	DISFLAY NAME	
	Full Access The full Access permission allows a delegate to open this mailbox and behave as the mailbox owner.	
		-

- 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.



Quarantine Admin			
general mailbox usage contact information organization ereal exidence	Field A: The field particular set dispets to used end from the makes. The message of apperts to how here sure by the tables sense. + -  (25 MENCEM Solid		
mailbox features member of MailTip	NY AIRCRAFYAIT	•	
<ul> <li>mailbox oblegation</li> </ul>	Sect on New 2 The first in the off previous dates the delayer to contend as both of the subject to be be any arrange set by a delayer inducts for the energy are of by the delayer solution of the endpoint on the off or endpoint on the off of the endpoint		
	DOLY MAK		
-	la Arona Dia Ma Annae paraminina aliane a sidengara ta apen titi multera and bahane an te multera mone. + ★ →		
	pan we . Reproved to the control of		
		Sine	Cancel

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 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



=		
仚	Home	
8	Recipients	$\sim$
	Mail flow	$\sim$
2	Roles	^
	Admin roles	
	Migration	
•I	Mobile	$\sim$
	Reports	$\sim$
Q	Insights	
品	Organization	$\sim$
Ē₽	Public folders	$\sim$
t €	Public folders Settings	~

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

Admin roles					
Admin role groups give users permissions to v Exchange admin center. Give users only the ac about managing role groups	view data, complete tasks, and use Powershell cmdlets in the ccess they need by assigning the least-permissive role. Learn more				
<sup>የ</sup> ቋ <sup>ል</sup> Add role group	18 items 🔎 Search =				
Role group ↑	Description				
Compliance Management This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.					
Discovery Management         Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.					

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



Disco	overy l	/lanagement	×
General Basics	Assigned	Permissions	
<b>Name</b> Discovery	Management		

5. Locate the ApplicationImpersonation role and select it.

Genera	Assigned Permissions			
Add or tasks ar	remove roles to the <b>Discovery</b> Ind resources that the members	Manage assigne	ement role group. Roles d to this role group can	define the manage.
	3 selected $ imes$ [	,∕⊃ Se	arch	=
	Role ↑		Default recipient scope	Default configu
	Address Lists	i	Organization	OrganizationCo
		$\bigcirc$	0:	News

General	Assigned	Permissions			
hese are f ole group	the admins as here.	signed to this role.	. You can add c	r remove admi	ns from this

- 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

#### STEP 7: CONFIGURE IDR TO PROVISION THE GROUP OF USERS

This step associates the Mailbox group you created in <u>Step 2</u>, 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.



≡		
ណ៍	Home	
8	Users	^
	Active users	
	Contacts	
	Guest users	
	Deleted users	
የደግ	Teams & groups	^
	Active teams & groups	
	Deleted groups	
	Shared mailboxes	
R	Roles	~
	Billing	~
٢	Settings	^
	Domains	
	Search & intelligence	
_	Org settings	
	Integrated apps	
	Partner relationships	
Þ	Setup	
	Show all	_

#### 4. Select Upload Custom App.

Home $>$ Integrated apps		🕗 Dark mode			
Integrated apps					
Discover: purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners. You can also deploy and manage Line-of-business add-ins developed within your organization. For advanced management of these apps go to the respective admin center or page : Azure Active Directory   SharePoint   Teams   Add-ins					
🗄 Get apps  주 Upload custom apps 🕐 Refresh	1 items 🔎 Searc	ch			

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



Upload custom app	Upload Apps to deploy
Users	Host Product
Deployment	Word, Excel, Powerpoint and Outlook $\sim$ $\bigcirc$
	Choose how to upload app
	Upload manifest file (.xml) from device
	choose file from your desktop Choose File
	Provide link to manifest file
	https://addin2.idr.gosecure.net/contentACCES Validate

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

Is this a test deployment? (i) No
Assign users
Just me (Globaltestadmin@teamstpxone.onmicrosoft.com)
Entire organization
• Specific users/groups
To be added
TPx IDR Users ×
Added 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 <u>Step 2</u> and the add in deployment in <u>Step 6</u>. 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 <u>Step 6</u> 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 <u>Step 3</u>.
- The other necessary permission, GoSecure IDR Prod Azure Admin, can be found within the <u>Azure Admin Center</u>. 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.

All services   All All Frontes Frontes Categories General Identity Security Hybrid + multicloud	Filter services       Azore Active Detectory       General (1) <sup>®</sup> Help + support        Identity (19)					
	Azure Active Directory  Azure AD Connect Health  Azure AD Connect Health  Azure AD Conditional Access  Azure AD Identity Protection  App proxy  Administrative units  D External Identities  Security (14)	Groups  Enterprise applications  Accure AD Privileged Identity Management  User settings  Security  Accure AD roles and administrators	Users  I clantity Governance  Aure AD Security  AD Connect  Terunt properties  Create oution Azure AD roles			

• From the Enterprise Applications section, the following applications display:

All services > Enterprise applications Enterprise applications   All applications Ty, Communications - Azure Active Directory								
40	< 🕂 New application 🕐 Refresh 🞍 Download (Preview)   🕕 Preview info   🎫 Columns   🖽 Preview features   🔗 Got feedback?							
Overview								
() Overview	Want to switch back to the legacy Ent	terprise Apps search experience? Click to	o leave the preview. $\rightarrow$					
X Diagnose and solve problems	View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.							
Manage								
All applications	Search by application name or object	Application type == E	interprise Applications X Applications status =	== Any × Application visibility == Any	X <sup>+</sup>			
	3 applications found							
Application proxy	Name	↑↓ Object ID	Application ID	Homepage URL	Created on	↑↓		
User settings	MW Modern Workplace Tools	23b0313d-6c18-4d57-b56f-	c32b9db01a66 fe6aa35b-7da8-44fd-a44e-e2d4b	bafbdab5	3/15/2022			
Collections	GoSecure IDR PROD 0365	56e54f92-a799-48c7-934a-	c342c7d804a3 830e4de6-8192-45f8-b2fe-2b725	57a22b04 https://www.gosecure.net	3/18/2022			
Security	GoSecure IDR PROD Azure Adr	min fc58677c-57b9-4ff6-98da-3	f31e0e6a645 3be24644-4ec6-4419-ac69-e696	1a3a8b8e https://www.gosecure.net	3/18/2022			

- o GoSecure IDR PROD 0365
  - These permissions display when TPx initially logs the global administrator into the GoSecure Portal in <u>Step 4</u>.
- GoSecure IDR Prod Azure Admin
  - These permissions display when TPx initially configures the GoSecure IDR Admin Portal.