Inbox Detection & Response

GoSecure

Provisioning Guide for O365

Overview

The IDR System requires awareness of what users are configured to use the service, and also must have access to these users mailboxes in order to perform its function. This document explains what access is required and how that access can be administered.

NOTE: *If you are using an on-premises Exchange server instead of Office365, you will want to refer to the IDR On Premise provisioning documentation instead.*

Administrative Configuration

Overview

The following configuration steps will be performed:

1. Identify or create a single group that contains all the users you wish to activate for IDR
2. Identify or create an administrative level user who has access to the members of the above group's mailboxes
3. Grant the IDR application access to the user mailboxes using the administrative account from step 2.
4. Configure IDR to activate users from the group in step 1.
5. Install an outlook add-in for this group using the Microsoft 365 Admin Console

Step 1: Identify or create a group of users for IDR

IDR uses an exchange group to identify which users should have access to the system. Only users of this group will be able to use the service. This group will be used both in the IDR configuration screen as well as when you deploy the outlook add-in in the Microsoft 365 Admin Center.

Choose a group name, in this document we will call it "IDR Users".

Login to the Microsoft 365 Admin Center with an administrative account capable of creating groups. Create a new group (Distribution Group is preferred) and give it the name "IDR Users". You do not need to add Group Owners for the purposes of IDR. Give it an email address of your choosing – this will not be used in IDR. You do not need to allow people outside of your organization to send to this email address either.

Step 2: Configure a Global Administrator user for IDR

To perform its function, IDR requires an O365 account (Azure Portal) with "Application Administration" permission. Additionally, this account will need to have "Full Access" impersonation rights on the mailboxes which belong to the IDR Users group identified above.

- **Create an account (here we will use "IDR Admin" and assign to it the role "Application Administration"**
  - Log in aad.portal.azure.com
  - Click on Users
  - Double click on the user (IDR Admin) from all users
  - Click "Assigned Roles"
  - Click on "Add Assignment"
  - Click on the "Select Role" dropdown list
  - Choose "Application administration"

Provisioning Guide for O365

- **For each user that is placed in the IDR Users group (i.e. each user licensed for IDR), you must allow the "IDR Admin" user above to have mailbox delegation rights to "Full Access" for this user.**
- Go to User, then Edit Exchange Properties, Mailbox Delegation, and add the "IDR Admin" to Full Access list
- Repeat for each user in the Group. (*GoSecure can provide a powershell script to support automating this process*)

Step 3: Grant the IDR application access to the mailboxes

During this step, you will need to log into your Microsoft 365 Account that as the "IDR Admin" user from above.

- Visit GoSecure Inbox Detection & Response Central Admin page, and navigate to the System Settings tab.
- Click through on "**Office 365 Admin Authorization**" in the "**EWS Authentication: Section**".
- You will be prompted to login – Do so as the "IDR Admin" user created above.
- Once logged in, review the permissions requested and grant consent for your organization. (Note important to grant for organization).

Step 4: Configure IDR to provision the group of users

The final step in provisioning is to make IDR aware of which users are licensed to use the service. This involved providing IDR with the group information determined in Step 1 above.

- Visit GoSecure Inbox Detection & Response Central Admin page, and navigate to the User Experience tab.
- Click on "Add Group" – or if a group has already been added click on the ellipses to edit the group.
- Provide the group email address – in our case "IDR Users" and confirm.
- Shortly after this, you should see IDR iterating through the list of users in this group, provisioning them in its database.
- Take note of the Add-in URL from the User Experience page, you will need it in the next step.

Step 5: Install the outlook add-in in Microsoft 365 Admin Center

[Reference: *https://docs.microsoft.com/en-us/microsoft-365/admin/manage/test-and-deploy-microsoft-365-apps?view=o365-worldwide#deploy-an-office-add-in-using-the-admin-center*]

Before starting, make sure you have the Add-in URL you collected from the prior step.

Next, in the Microsoft 365 Admin Center,

- Visit Settings / Integrated Apps,
- Choose Upload Custom App,
- Select Provide Link to Manifest File, then paste in the URL from above and validate.
- On the next page, select to deploy to Specific Users/ Groups; enter the group from above, in our case IDR Users. Click next
- Accept the permissions request and deploy the app
- Confirm the deployment on the next page.

NOTE: The outlook add-in may not be visible in the users' mailboxes for several hours. This is a Microsoft limitation and expected behavior with office add-ins.