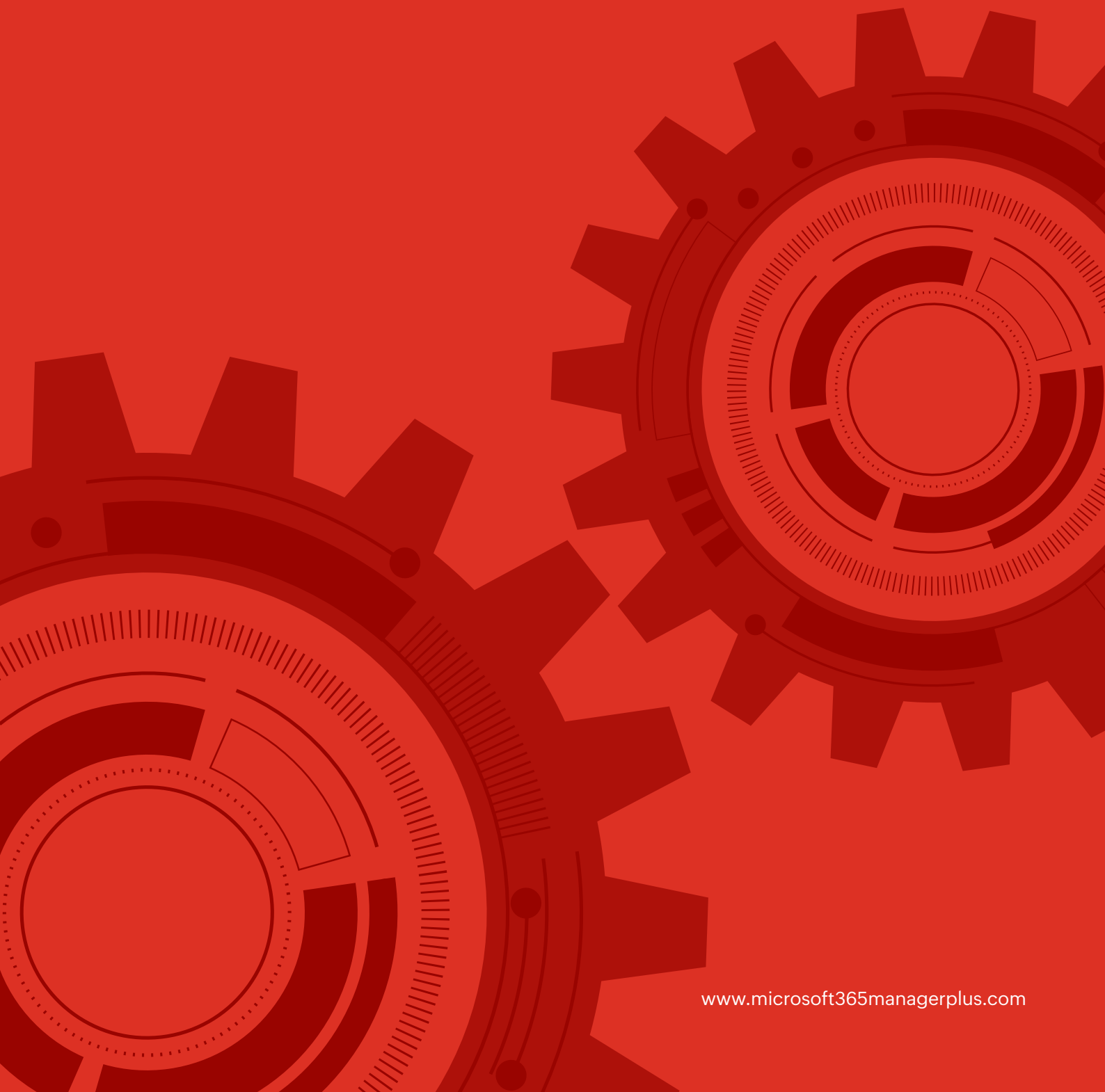
ManageEngine
M365 Manager Plus

Microsoft 365 Tenant Configuration



www.microsoft365managerplus.com

Table of Contents

Microsoft 365 tenant configuration 2

Automatic Microsoft 365 tenant configuration 2

Steps to modify REST API permissions 4

Manual Microsoft 365 tenant configuration 6

- Steps to create an Azure AD application 7
- Steps to configure an Azure application in M365 Manager Plus 11
- Steps to configure a service account in M365 Manager Plus 11

Steps to modify a Microsoft 365 tenant 12

How to configure an MFA-enabled service account 12

- Steps to configure Trusted IPs 12
- Steps to configure Conditional Access 12

Appendix 13

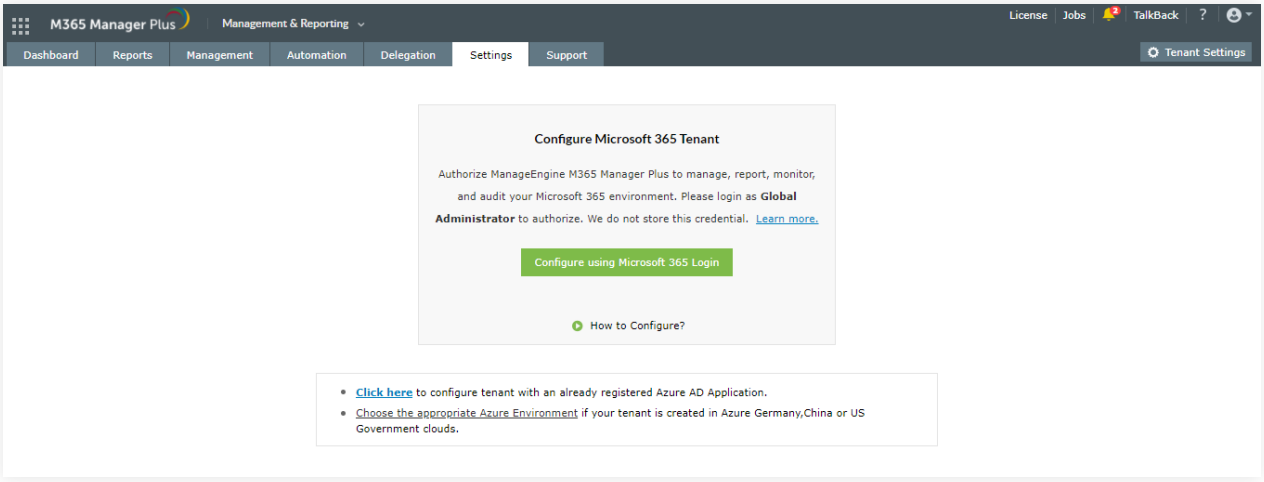
- Minimum scope 13

Microsoft 365 tenant configuration

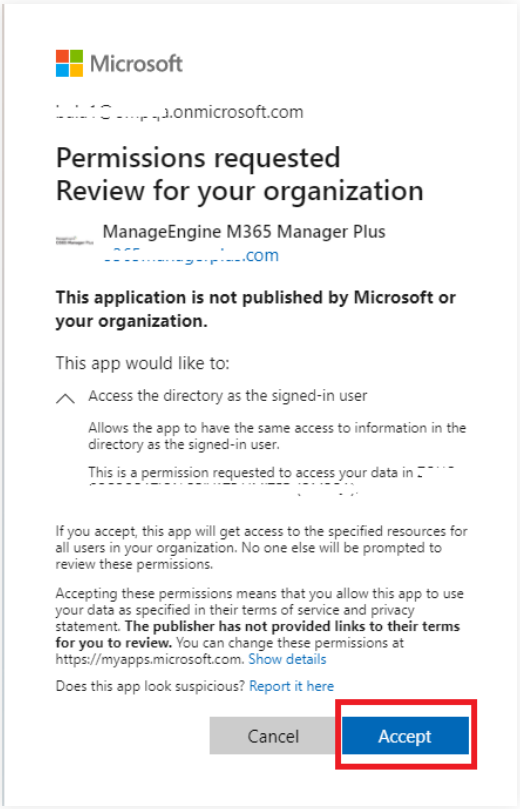
When you log in to M365 Manager Plus for the first time, you will be required to configure a tenant to use the tool. Once you log in, you will be automatically redirected to the tenant configuration page. If you want to configure additional tenants, the Tenant Settings option can be found in the top-right corner of the M365 Manager Plus window.

Automatic Microsoft 365 tenant configuration

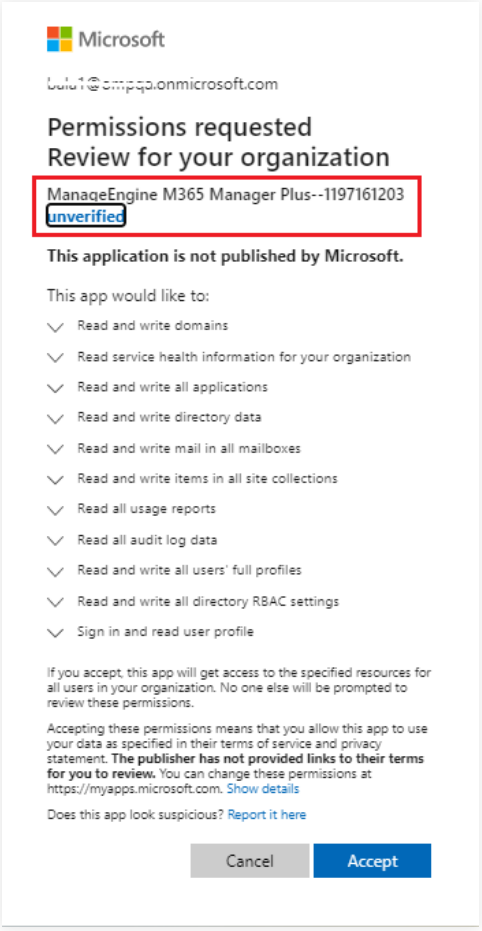
1. Log in to M365 Manager Plus as an administrator. The default username and password are admin and admin respectively.
2. Choose the **Tenant Settings** option found in the top-right corner.
3. If you are configuring your first tenant, click **Configure using Microsoft 365 Login**. Otherwise, choose **Add Tenant**, then click **Configure using Microsoft 365 Login.**



4. Click on **Proceed** in the pop-up that appears.
5. You will be diverted to the Microsoft 365 login portal. Enter the credentials of a Global Administrator account.
6. Click **Accept.**



7. An application and service account for M365 Manager Plus will be created automatically.
   You will now see a page that displays the list of permissions the application needs.
   Please note down the application name, which is shown at the top. You will need this later.

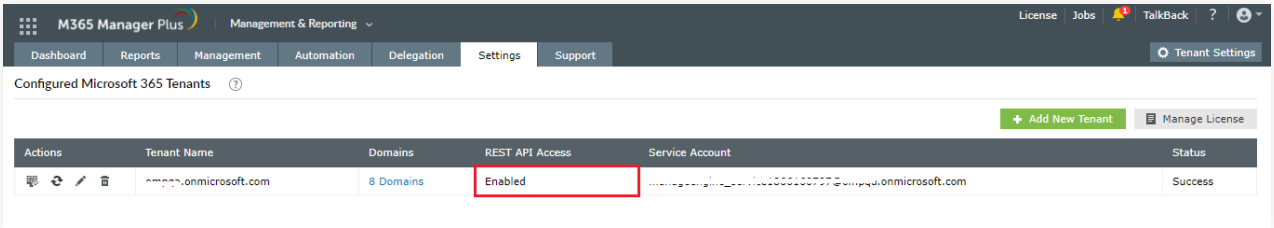


8. Go through the list and click **Accept.**

Note: If you do not want to provide all the required permissions, please configure your tenant manually.

You can also choose to configure your tenant now and modify the permissions later.

9. You will now be redirected to the M365 Manager Plus console, where you can see that REST API access is enabled for the account you configured. If REST API access is not enabled, you have to do it manually.

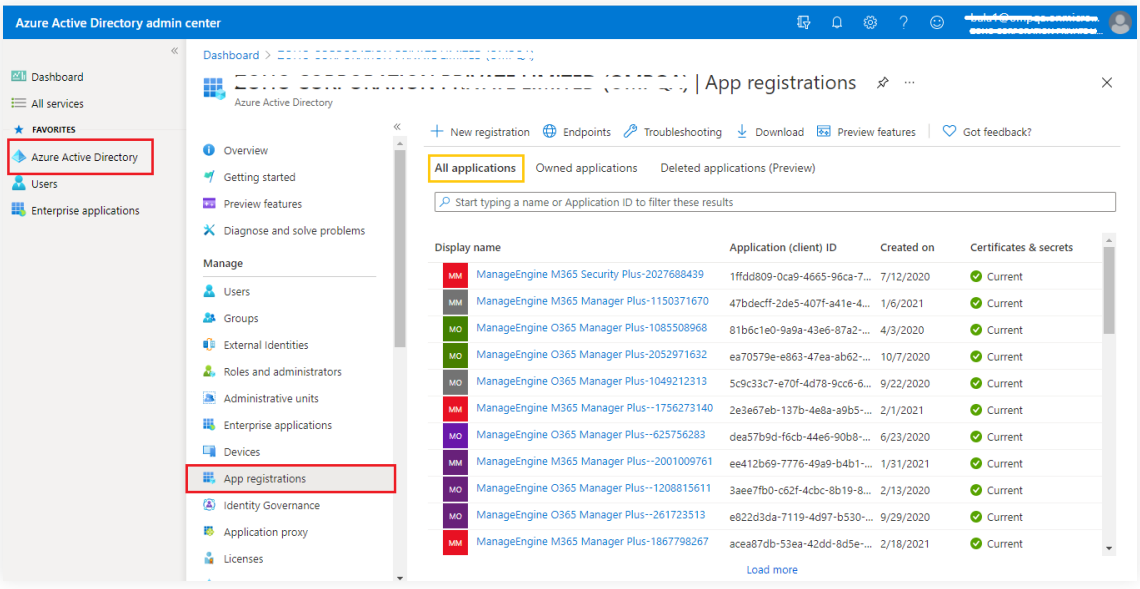


Steps to modify REST API permissions

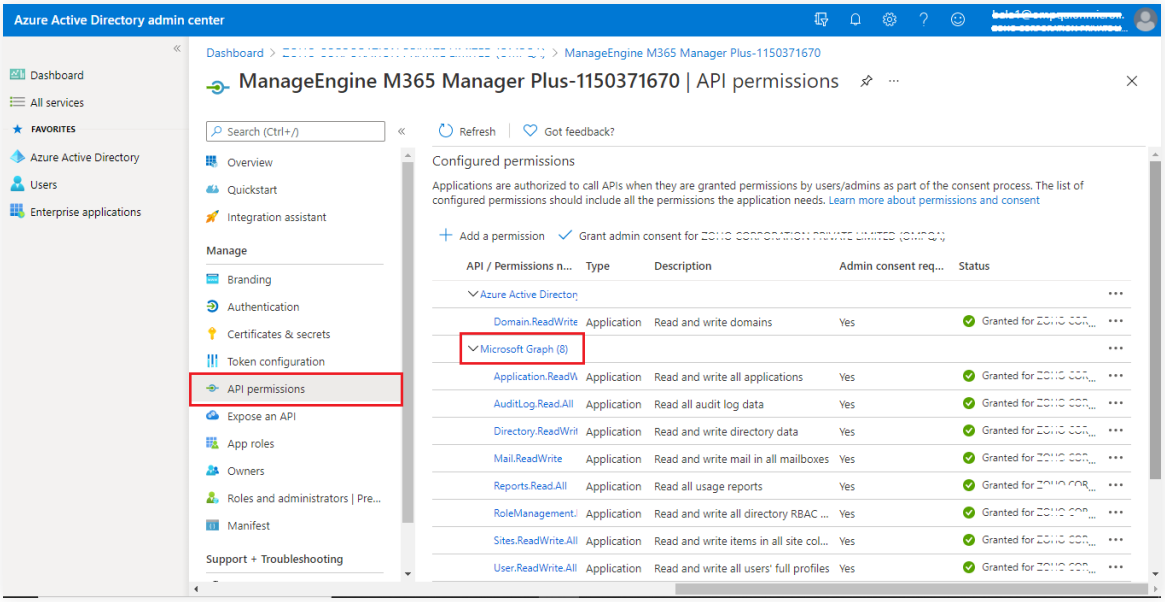
Though we suggest providing all the recommended permissions, organizational requirements may not allow this. In this section, you will learn how to modify the REST API permissions for an already configured tenant. If you are looking for a way to configure a tenant with only the permissions you require, please configure it manually.

Prerequisite: The tenant has been successfully configured in M365 Manager Plus and REST API is enabled for it.

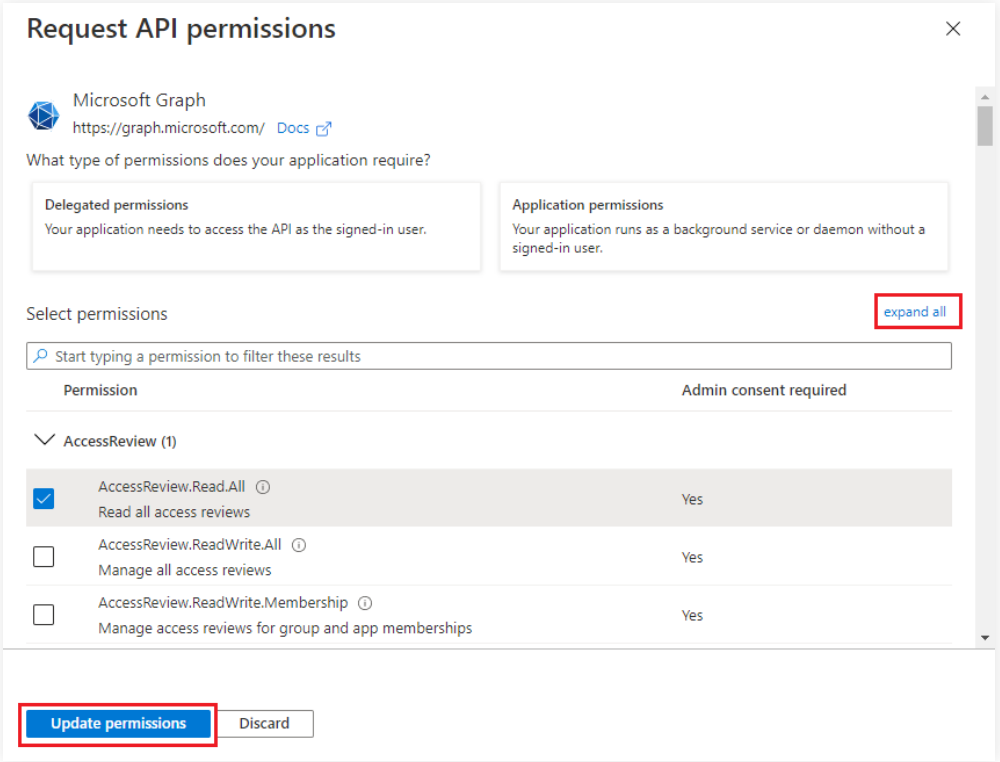
1. Log in to the Azure AD admin center.
2. Click Azure **Active Directory** from the left pane.
3. Choose **App registration** under Manage.
4. Select **All applications**.



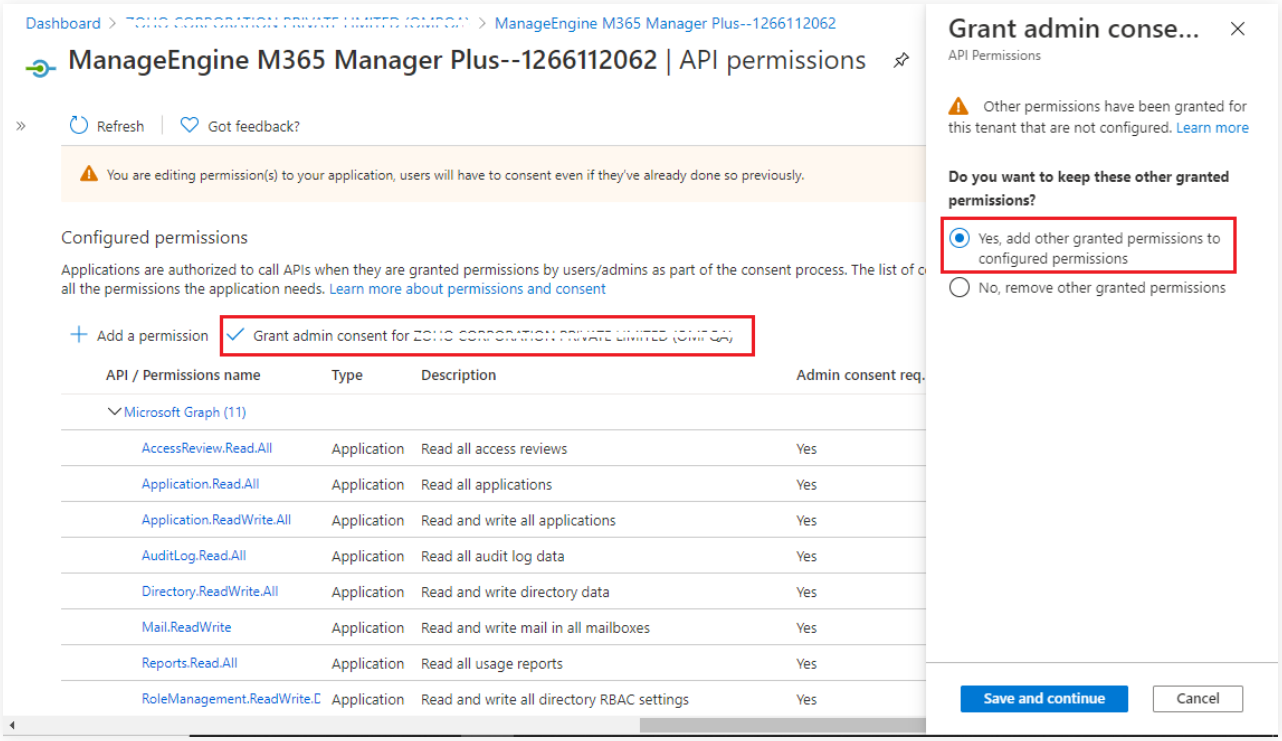
5. Search for the application name from step 7 of the previous section and click it.
6. Select **API Permissions** under Manage.
7. Choose **Microsoft Graph.**



8. Click **expand all** to view all the permissions already granted to this application.
9. Add, remove, or modify permissions as per your requirements.
10. Click **Update permissions.**



11. Select the **Grant permission for domain_name** option found at the top of the permissions table.
12. Choose **Yes, add other granted permissions to configured permissions** in the window that appears.



13. Click **Save and Continue > Grant admin consent > Yes.**
14. You have now successfully modified the permissions required by the REST API application.

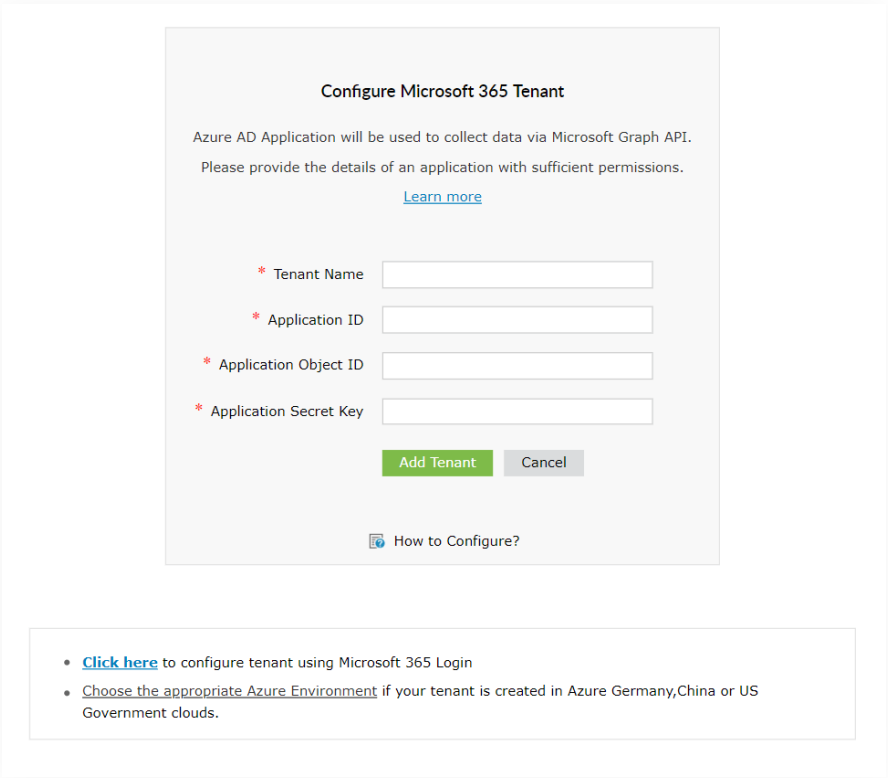
Manual Microsoft 365 tenant configuration

If the automatic configuration was not successful due to permission issues, the tenant must configured manually. To do that, select Click here to configure with an already existing Azure AD application. Please note that you can also opt to configure manually and skip the automatic configuration altogether with the option provided.

Prerequisite: A service user account with at least View-Only Organization Management, View-Only Audit Logs, and Service Administrator permissions. Click here to learn how to create a Microsoft 365 service account.

Manual tenant configuration involves the following three steps:

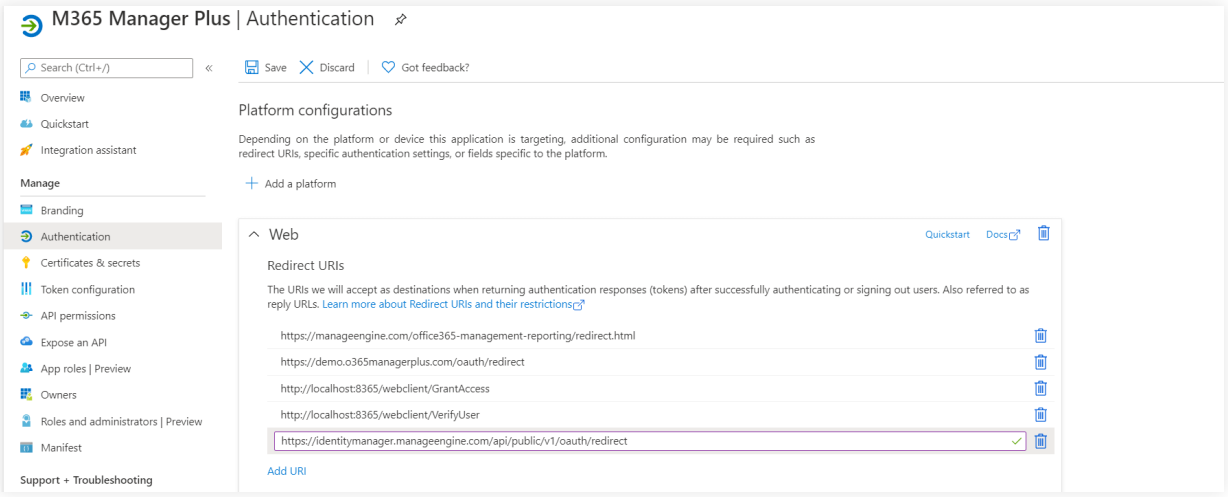
1. Create an Azure AD application
2. Configure the Azure AD application in M365 Manager Plus
3. Configure a service account in M365 Manager Plus



Steps to create an Azure AD application

1. Sign in to the Azure AD portal using the credentials of a Global Administrator account.
2. Select **Azure Active Directory** from the left pane.
3. Select **App registrations.**
4. Click **New registration.**
5. Provide a **Name** for the M365 Manager Plus application to be created.
6. Select a supported account type based on your organizational needs.
7. Leave **Redirect URI (optional)** blank; you will configure it in the next few steps.
8. Click **Register** to complete the initial app registration.
9. You will now see the Overview page of the registered application.
10. Click **Add a Redirect URI.**
11. Click **Add a platform** under Platform configurations.
12. In the Configure platforms pop-up, click **Web** under Web applications.
13. In the **Redirect URI** field, enter **http://localhost:port_number/webclient/VerifyUser.**
    For example, http://localhost:8365/webclient/VerifyUser or https://192.345.679.345:8365/webclient/VerifyUser.
14. You can leave the Logout URL and Implicit grant fields empty. Click **Configure.**
15. On the Authentication page, under Redirect URIs, click **Add URI.**
16. Enter **http://localhost:port_number/webclient/ GrantAccess** as the Redirect URI.
    For example, http://localhost:8365/webclient/GrantAccess or https://192.345.679.345:8365/webclient/GrantAccess.

17. Again click **Add URI** to add the below REDIRECT URIs in the subsequent rows. Please note that for **users with M365 Manger Plus build 4409 or higher, REDIRECT URIs (b) and (c) are optional.**
    a. https://identitymanager.manageengine.com/api/public/v1/oauth/redirect
    b. https://demo.o365managerplus.com/oauth/redirect
    c. https://manageengine.com/microsoft-365-management-reporting/redirect.html



Note: The REDIRECT URI must adhere to the following:

- It must be fewer than 256 characters in length.
- It should not contain wildcard characters.
- It should not contain query strings.
- It must start with HTTPS or http://localhost.
- It must be a valid and unique URL.

  Based on the connection type (http/https) you have configured in M365 Manager Plus, the REDIRECT URI format varies.
- For http, the URI value is http://localhost:8365. Machine name or IP address cannot be used in place of localhost if http is used.
- For https, the URI value is https://192.345.679.345:8365 or https://testmachine:8365.

To find your machine's **IP**, open the **Command Prompt**, type **ipconfig**, and click **enter**. You can find your IPv4 Address in the results shown.

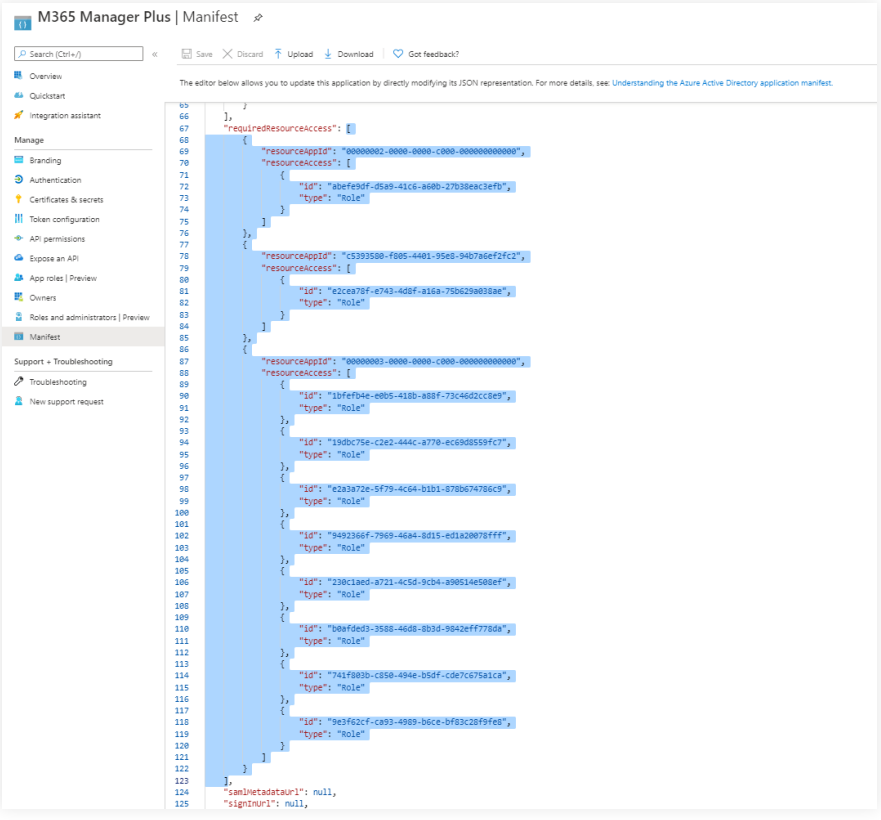
18. Click on **Save.**
19. Click on **Manifest** in the left pane.
20. Look for requiredResourceAccess array in the code.
21. Copy the entire contents from this file and paste them into the section highlighted in the image below. If you want to modify the permissions to be provided, skip this step and follow the steps mentioned in this section.

Note:

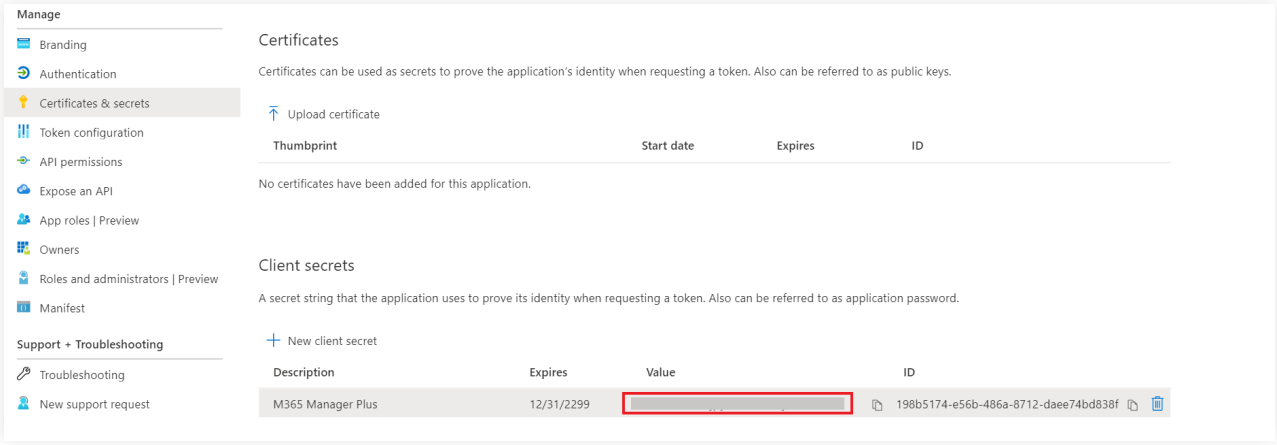
- If your tenant is created in **Azure Germany,** copy the entire content in this file and paste it in the section that is highlighted in the image below.
- If your tenant is created in **Azure China**, copy the entire content in this file and paste it in the section that is highlighted in the image below.

```
        },
        {
            "url": "http://localhost:8365/webclient/VerifyUser",
            "type": "Web"
        }
    ],
    "requiredResourceAccess": [
        {
            "resourceAppId": "00000003-0000-0000-c000-000000000000",
            "resourceAccess": [
                {
                    "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
                    "type": "Scope"
                }
            ]
        }
    ],
    "samlMetadataUrl": null,
    "signInUrl": null,
    "signInAudience": "AzureADMyOrg",
    "tags": [],
    "tokenEncryptionKeyId": null
```

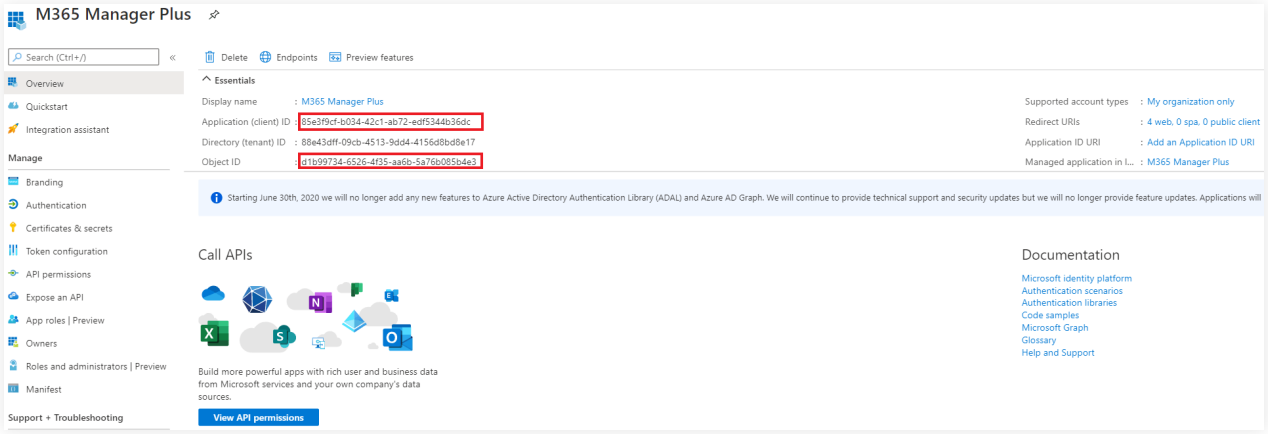
Note: Copy-paste content only from the open square bracket to the closed square bracket. Ensure that all punctuation marks are retained correctly. Once you have pasted the file, it should look like the image below.



22. Click **Save.**
23. Click **API permissions** from the left pane.
24. In the **Configured permissions** section, click ✔ **Grant admin consent for <your_company_name>.**
25. Click **Yes** in the pop-up that appears.
26. Click **Certificates & secrets** from the left pane.
27. Under the Client secrets section, click **New client secret.**
28. This section generates an app password for M365 Manager Plus. In the **Description** field of the pop-up, provide a name to identify the app to which the password belongs.
29. Choose when the password should expire.
30. Click **Add.**
31. Copy the string under Value and save it. This is the **Application Secret Key**, which you will require later.



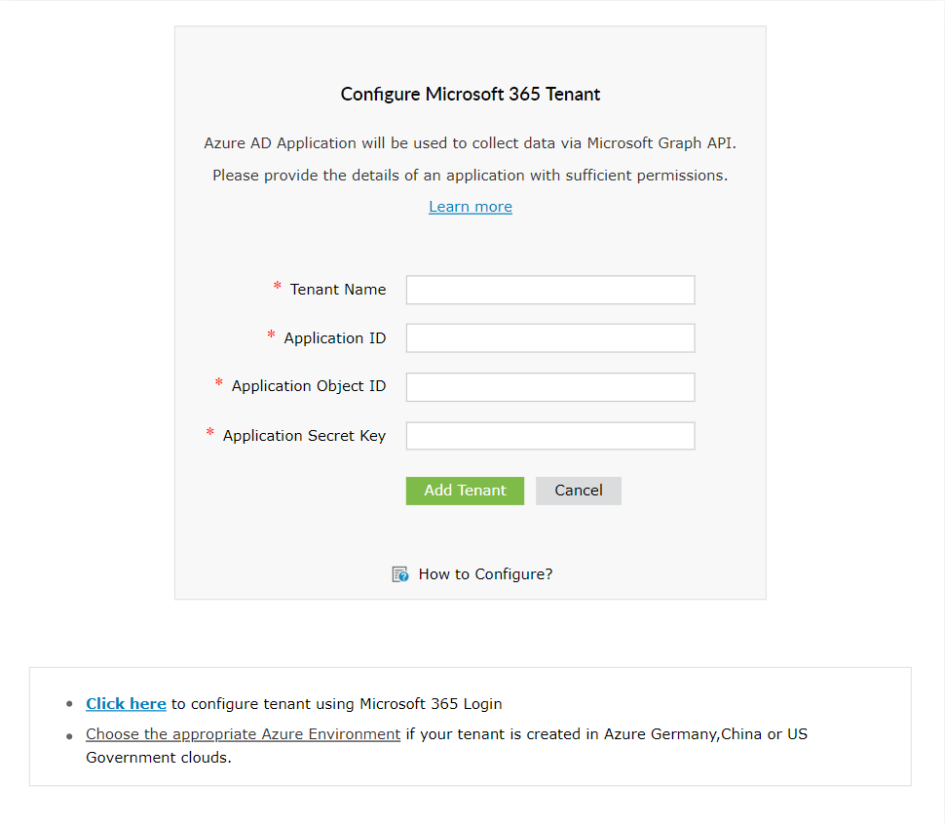
32. Now go to the **Overview** section in the left pane.
33. Copy the **Application (client) ID** and **Object ID** values and save them. You will need these values to configure your tenant in the M365 Manager Plus portal.



34. Refer to this table to learn about the roles that must be assigned to the application.

Steps to configure an Azure application in M365 Manager Plus

35. Return to the M365 Manager Plus console where you have the pop-up.



36. Enter your **Tenant Name**. For example, test.onmicrosoft.com.
37. Paste the **Application ID** and **Application Object ID** values copied in Step 33 into the respective fields.
38. For the **Application Secret Key**, paste the value copied in Step 31.
39. Click **Add Tenant**.
40. You should now see that REST API access is enabled for the account you configured.

Steps to configure a service account in M365 Manager Plus

1. Now the service account must be configure. In order to do so, click on the edit option under the **Actions** column.
2. Click on the **Edit** icon found near Service Account Details.
3. Enter the credentials of the service account you need to configure in the respective fields.
4. Click on **Update** and close the pop-up window.

Note: If your service account is MFA-enabled, please check this section.

Steps to modify Microsoft 365 tenant

- Click on the **Tenant Settings** option found at the top right corner.
- You will see the list of Microsoft 365 tenants configured with M365 Manager Plus.
- Under the **Actions** column, click on corresponding to the tenant you need to modify.
- Click on ✎ adjacent to **Application Details/Service Account Details** to modify the corresponding values.
- Choose **Update** once you have made the changes.

How to configure an MFA-enabled service account

If your service account is MFA-enabled, you need to use either the Conditional Access or Trusted IP feature in Microsoft 365 to bypass MFA. Once you have configured one of these features, proceed to configure the service account in M365 Manager Plus.

Note: To use conditional access, you need **Azure AD Premium P1** license.

Steps to configure Trusted IPs

- Login to portal.azure.com using your global admin credentials.
- Click on **Azure Active Directory** under Azure services.
- Choose **Security** from the left pane.
- Click on **MFA** under the Manage category in the left pane.
- Choose the **Additional cloud-based MFA settings** option.
- In the new window that opens, go to the **trusted ips** section.
- Select the **Skip multi-factor authentication for requests from federated users on my intranet** option.
- In the text box, enter the IP address of the machine in which you have installed M365 Manager Plus.
- Click on **Save.**

Note: To use Conditional Access or Trusted IPs, you need an **Azure AD Premium P1** license.

Steps to configure Conditional Access

In this section, you will learn how to create a policy to enforce MFA and exclude M365 Manager Plus users so they do not have to undergo multiple authentication.

- Login to portal.azure.com using your global admin credentials.
- Click on **Azure Active Directory** under **Azure services.**
- Choose **Security** from the left pane.
- Click on **Conditional Access** under the **Protect** category in the left pane.
- Click on **New Policy.**
- Provide a name for the policy.

- Click on the **Users and groups** option.
- Select the **Exclude** tab.
- Select the **Users and groups** check box, and choose the M365 Manager Plus users for whom MFA must not be enforced.
- Click on **Select.**
- Under the **Access controls** section, click on **Grant.**
- Select the **Grant access** radio button, and **Require multi-factor authentication** check box.
- Click **on Select.**
- Click on **Create** and the **Save.**

Appendix

Minimum scope

The roles and permissions, or minimum scope, required by a service account configured for M365 Manager Plus are listed below.

Table 1: Roles and permissions required by the service account.

Module	Role Name	Scope
Management	User Administrator	Manage users, contacts and groups.
	Privileged Authentication Administrator	Reset password, block or unblock administrators.
	Privileged Role Admin	Manage role assignments in Azure Active Directory.
	Exchange Administrator	Update mailbox properties
	Teams Service Admin	Manage Microsoft Teams
Reporting	Global Reader	Get reports on all Microsoft 365 services
	Security Reader	Get audit logs and mailbox reports.
Auditing and Alerting	Security Reader	Get audit logs and sign-in reports
Monitoring	-	-
Content Search	-	-

Note:

- If an Azure AD application is not configured for M365 Manager Plus, the Service Admin role is
- required for the Monitoring feature.

  An Azure AD application needs to be configured for M365 Manager Plus in order to use the Content Search feature.

The roles and permissions, or minimum scope, required by an Azure AD application configured for M365 Manager Plus are listed below.

Table 2: Roles and permissions required by the Azure AD application.

Module	API Name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	Create, modify, delete, or restore users.
		Group.ReadWrite.All	Create, modify, delete, or restore groups. Add or remove group members and owners.
Reporting	Microsoft Graph	User.Read.All	Get user and group member reports.
		Group.Read.All	Group reports.
		Contacts.Read	Get contact reports.
		Files.Read.All	Get OneDrive for Business reports.
		Reports.Read.All	Get usage reports.
		Organization.Read.All	Get license detail reports.
		AuditLog.Read.All	Get audit log-based reports.
	Azure Active Directory Graph	Domain.Read.All	Get domain-based reports.
Auditing and Alerting	Microsoft Graph	AuditLog.Read.All	Get audit reports and alerts.
Monitoring	Office 365 Management APIs	ServiceHealth.Read	Get health and performance reports.
Content Search	Microsoft Graph	Mail.Read	Get content search reports.