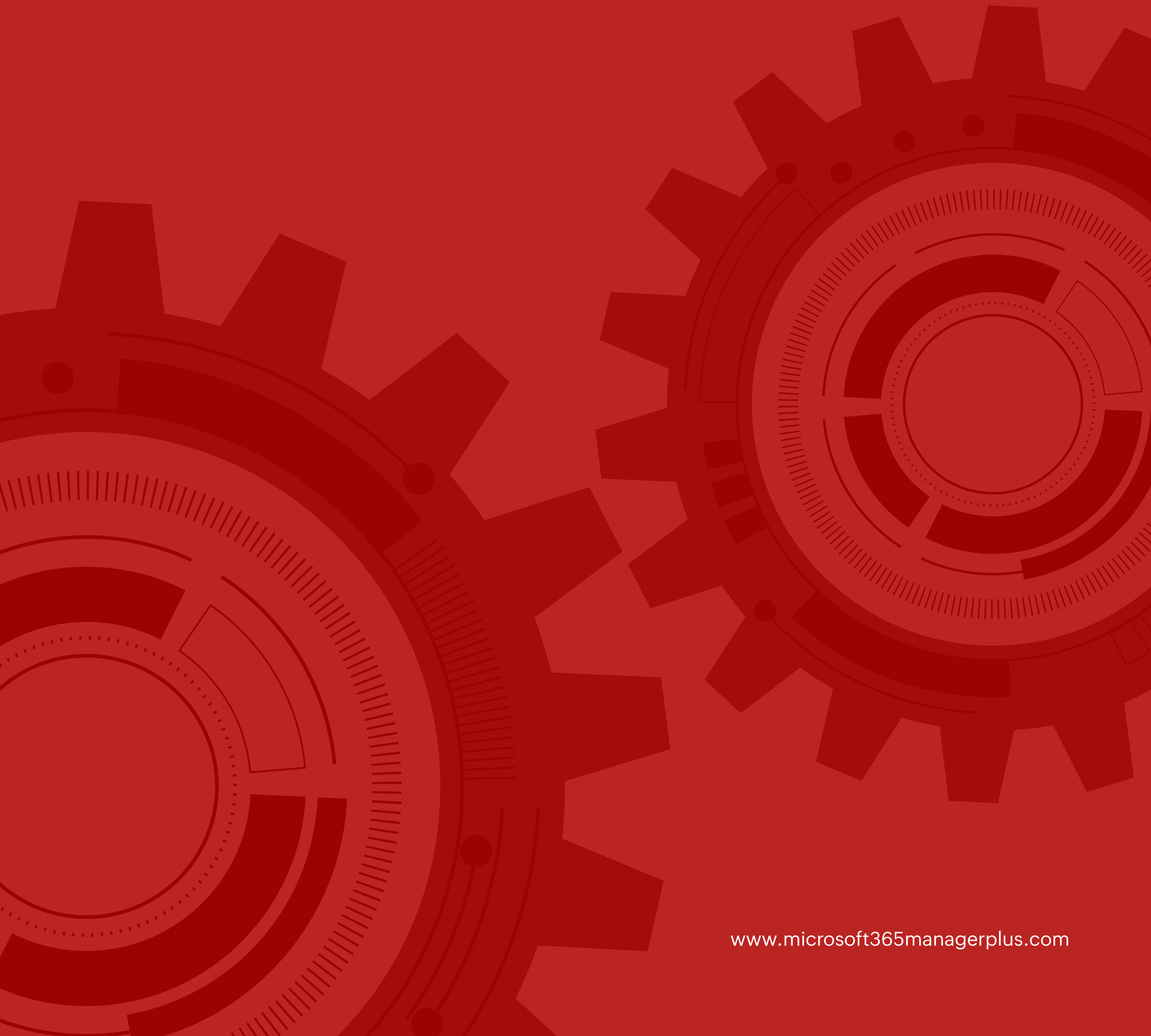
ManageEngine
M365 Manager Plus

Microsoft 365 Tenant Configuration



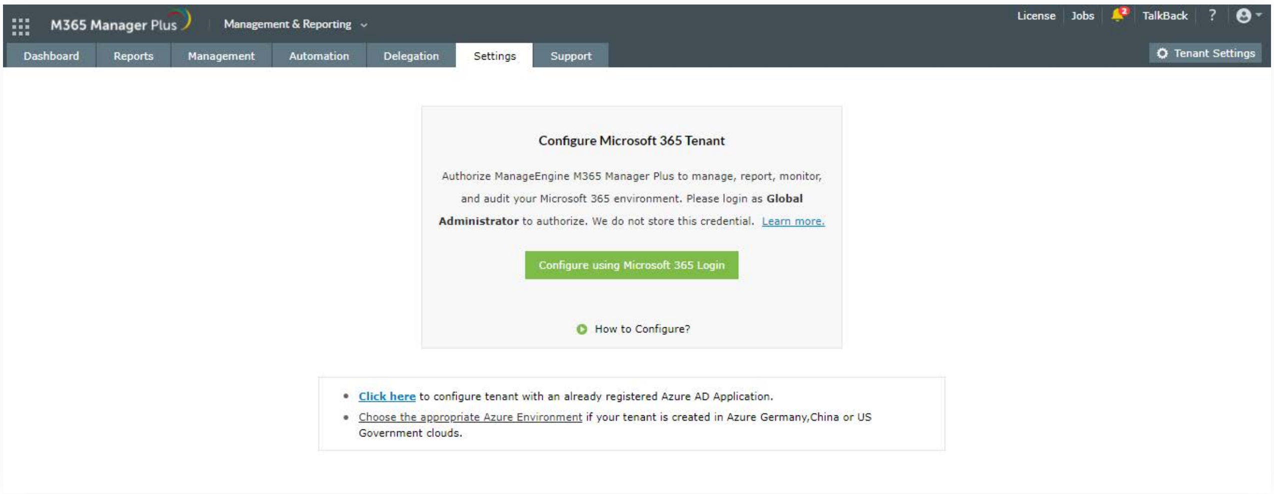
www.microsoft365managerplus.com

Table of Contents

When you open M365 Manager Plus for the first time, you will be required to configure a tenant to use the tool. Upon logging 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.**

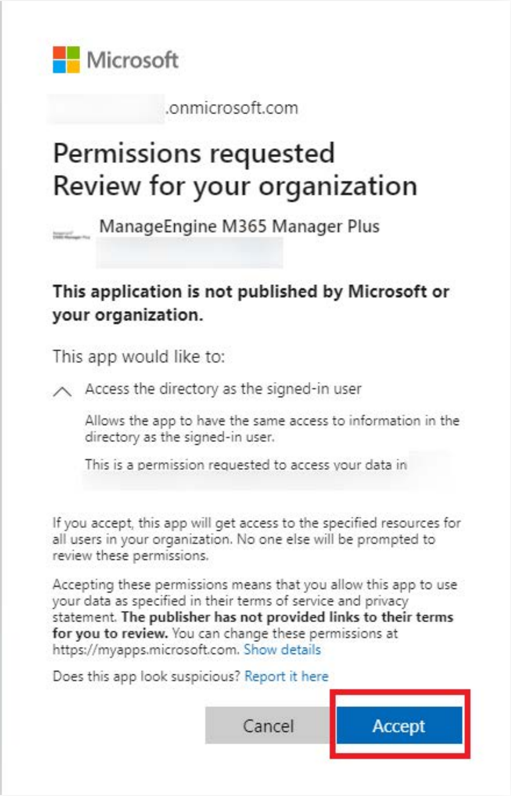


Configure Microsoft 365 Tenant

Authorize ManageEngine M365 Manager Plus to manage, report, monitor, and audit your Microsoft 365 environment. Please login as **Global Administrator** to authorize. We do not store this credential. Learn more.

- Click here to configure tenant with an already registered Azure AD Application.
- Choose the appropriate Azure Environment if your tenant is created in Azure Germany,China or US Government clouds.

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.**



Microsoft

.onmicrosoft.com

Permissions requested
Review for your organization

ManageEngine M365 Manager Plus

This application is not published by Microsoft or your organization.

This app would like to:

Access the directory as the signed-in user

Allows the app to have the same access to information in the directory as the signed-in user.

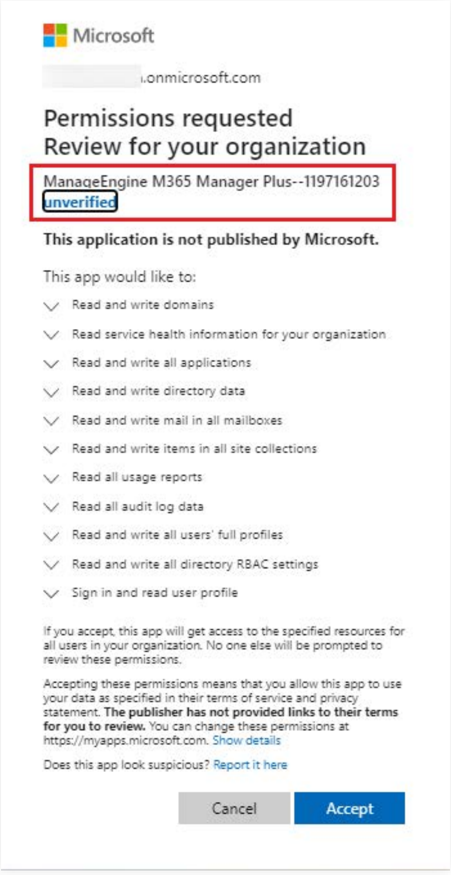
This is a permission requested to access your data in

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

7. An Entra application 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.



Microsoft

.onmicrosoft.com

Permissions requested
Review for your organization

ManageEngine M365 Manager Plus--1197161203
unverified

This application is not published by Microsoft.

This app would like to:

- Read and write domains
- Read service health information for your organization
- Read and write all applications
- Read and write directory data
- Read and write mail in all mailboxes
- Read and write items in all site collections
- Read all usage reports
- Read all audit log data
- Read and write all users' full profiles
- Read and write all directory RBAC settings
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

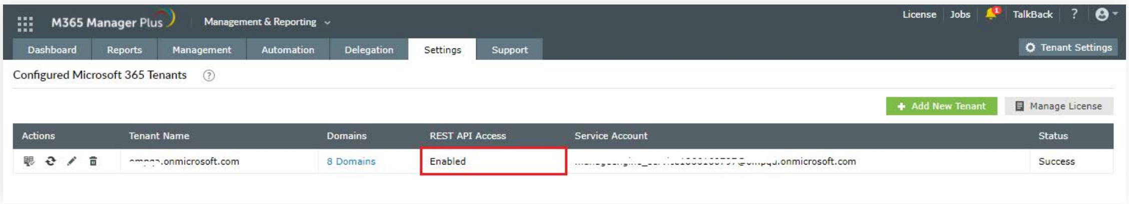
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

8. Go through the list of permissions 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 with full permissions now and modify the permissions later. using the Minimum Scope document for reference

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.



Configured Microsoft 365 Tenants

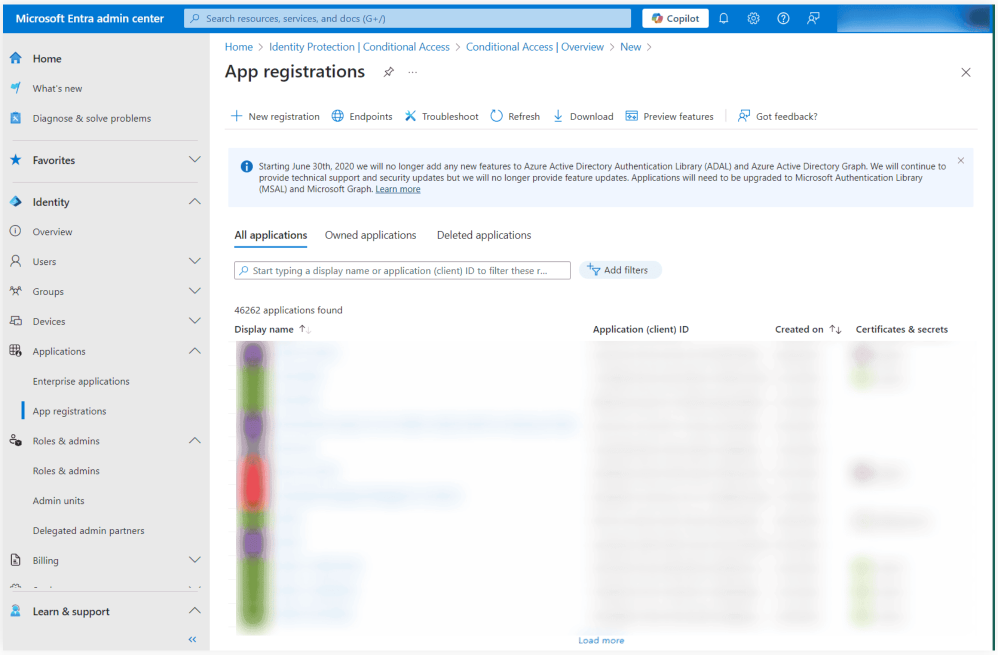
Actions	Tenant Name	Domains	REST API Access	Service Account	Status
	[redacted].onmicrosoft.com	8 Domains	Enabled	[redacted].onmicrosoft.com	Success

Steps to modify REST API permissions

Though we suggest providing all the recommended permissions, organizational policies 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 required for the features you want to use, here are the steps to do that manually.

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

1. Log in to the Microsoft Entra admin center using the credentials of a **Global Administrator** or any other user account with the permission to create Entra ID applications.
2. Navigate to **Identity > Applications > App registration.**
3. Select **All applications.**

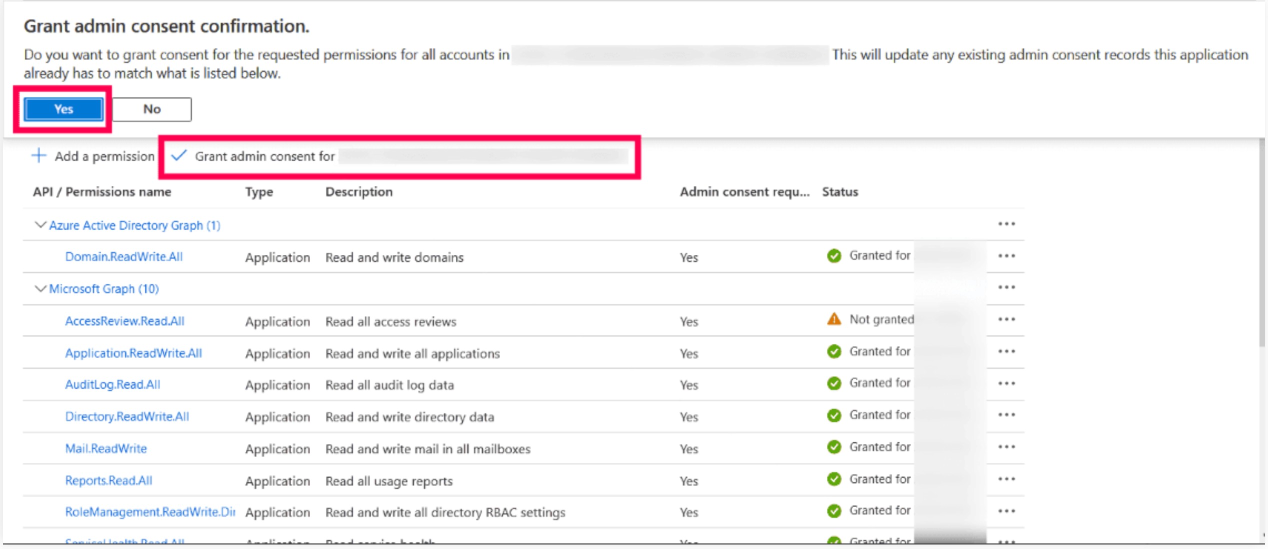


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

46262 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
[redacted]	[redacted]	[redacted]	[redacted]

4. Search for the application name that you configured and click it.
5. Select **API Permissions** under *Manage.*
6. Choose **Microsoft Graph.**

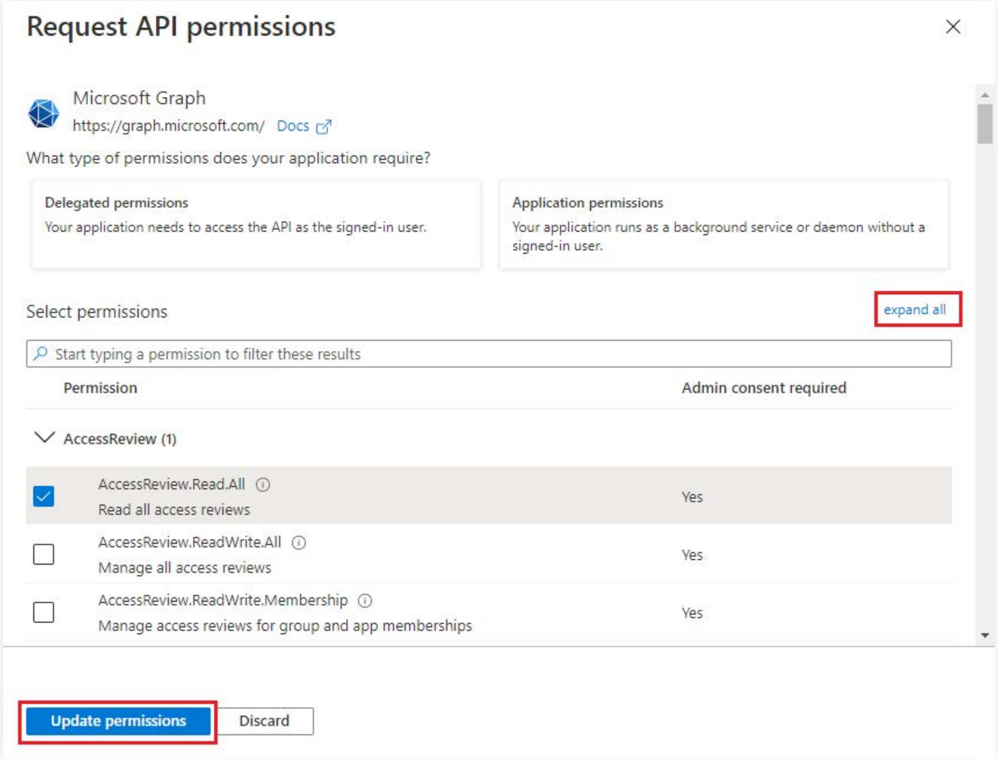


Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in [redacted] This will update any existing admin consent records this application already has to match what is listed below.

API / Permissions name	Type	Description	Admin consent requ...	Status
∨ Azure Active Directory Graph (1)				
Domain.ReadWrite.All	Application	Read and write domains	Yes	✓ Granted for [redacted]
∨ Microsoft Graph (10)				
AccessReview.Read.All	Application	Read all access reviews	Yes	⚠ Not granted [redacted]
Application.ReadWrite.All	Application	Read and write all applications	Yes	✓ Granted for [redacted]
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted for [redacted]
Directory.ReadWrite.All	Application	Read and write directory data	Yes	✓ Granted for [redacted]
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for [redacted]
Reports.Read.All	Application	Read all usage reports	Yes	✓ Granted for [redacted]
RoleManagement.ReadWrite.Di	Application	Read and write all directory RBAC settings	Yes	✓ Granted for [redacted]
ServiceHealth.Read.All	Application	Read service health	Yes	✓ Granted for [redacted]

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



Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

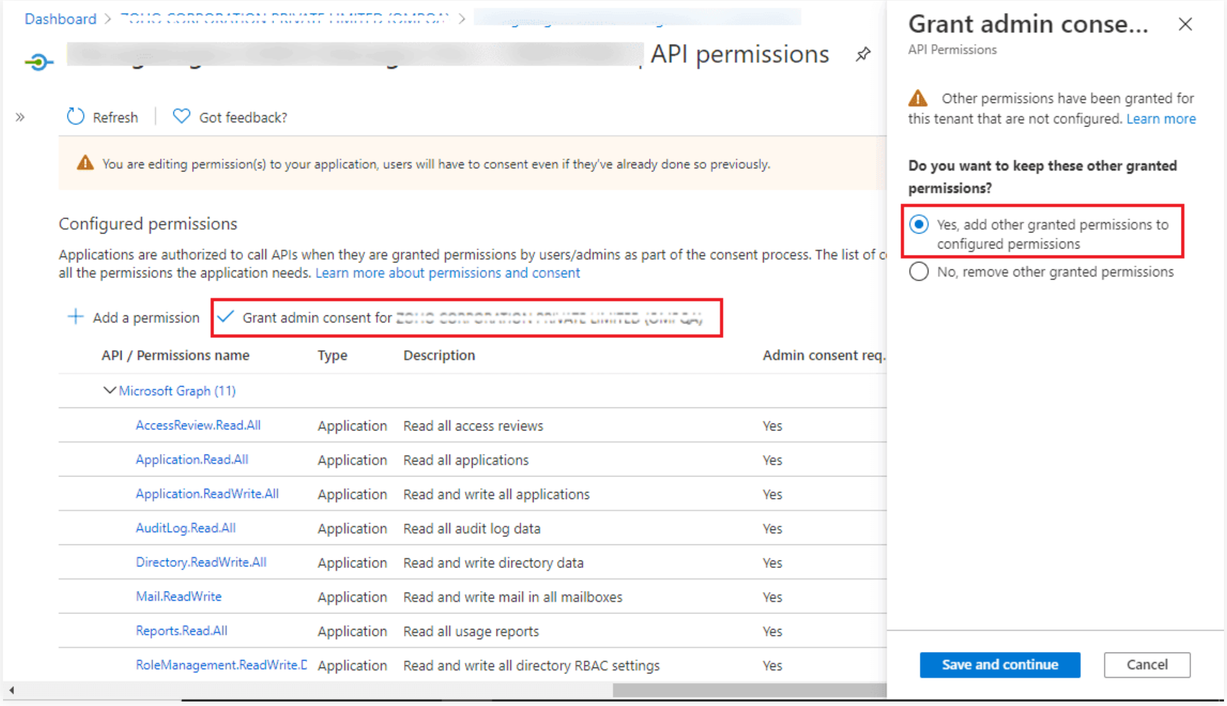
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

	Permission	Admin consent required
	∨ AccessReview (1)	
☑	AccessReview.Read.All ⓘ Read all access reviews	Yes
□	AccessReview.ReadWrite.All ⓘ Manage all access reviews	Yes
□	AccessReview.ReadWrite.Membership ⓘ Manage access reviews for group and app memberships	Yes

10. Select the **Grant admin consent for "domain_name"** option found at the top of the *Configured permissions* table.
11. Choose **Yes, add other granted permissions to configured permissions** in the Grant admin consent window that appears.
12. Click **Save and continue**, and in the pop-up that appears, click **Grant admin consent > Yes.**


Dashboard > [redacted] > [redacted]
[redacted] API permissions
Refresh
Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 c all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req.
Microsoft Graph (11)			
AccessReview.Read.All	Application	Read all access reviews	Yes
Application.Read.All	Application	Read all applications	Yes
Application.ReadWrite.All	Application	Read and write all applications	Yes
AuditLog.Read.All	Application	Read all audit log data	Yes
Directory.ReadWrite.All	Application	Read and write directory data	Yes
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes
Reports.Read.All	Application	Read all usage reports	Yes
RoleManagement.ReadWrite.D	Application	Read and write all directory RBAC settings	Yes

Grant admin conse...

API Permissions

Other permissions have been granted for this tenant that are not configured. Learn more

Do you want to keep these other granted permissions?

● Yes, add other granted permissions to configured permissions

○ No, remove other granted permissions

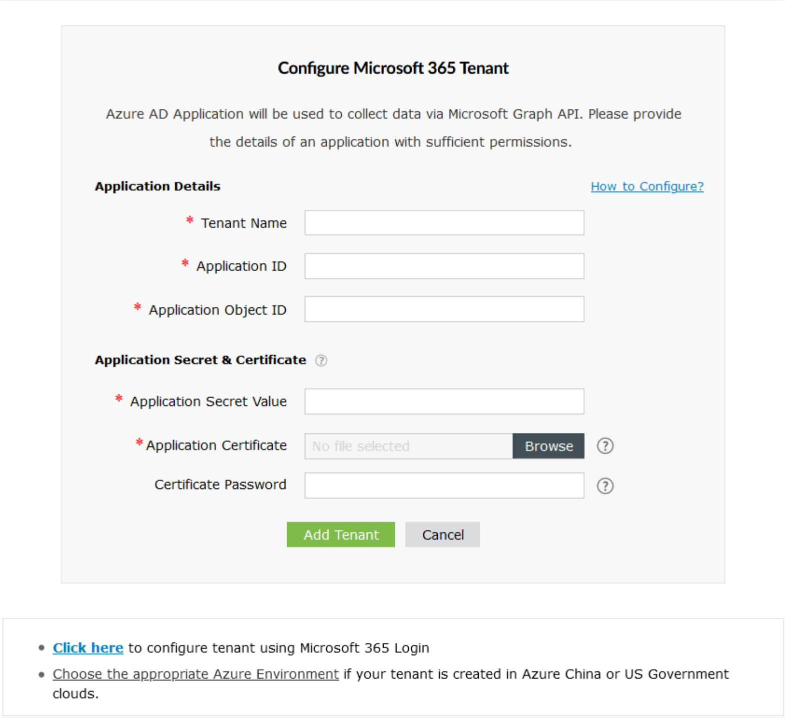
You have now successfully modified the permissions required by the REST API application.

Manual Microsoft 365 tenant configuration

If the automatic configuration was not successful due to permission issues, the tenant must be 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 the tenant manually and skip the automatic configuration altogether with the option provided.

Manual tenant configuration involves the following three steps:

1. Create an Entra application
2. Configure the Entra application in M365 Manager Plus



Configure Microsoft 365 Tenant

Azure AD Application will be used to collect data via Microsoft Graph API. Please provide the details of an application with sufficient permissions.

Application Details

How to Configure?

* Tenant Name

* Application ID

* Application Object ID

Application Secret & Certificate

* Application Secret Value

*Application Certificate No file selected Browse

Certificate Password

- Click here to configure tenant using Microsoft 365 Login
- Choose the appropriate Azure Environment if your tenant is created in Azure China or US Government clouds.

Steps to create an Entra application

1. Log in to the Microsoft Entra admin center using the credentials of a **Global Administrator** or any other user account with the permission to create Entra applications.
2. Navigate to **Identity > Applications > App registration.**
3. Click **New registration.**
4. Provide a **Name** for the M365 Manager Plus application to be created.
5. Select a supported account type based on your organizational needs.
6. Leave **Redirect URI (optional)** blank; you will configure it in the next few steps.
7. Click **Register** to complete the initial app registration.
8. You will now see the *Overview* page of the registered application.
9. Navigate to **Authentication** in the side pane.
10. Click **Add a platform** under *Platform configurations.*
11. In the Configure platforms pop-up, under *Web applications*, click **Web.**
12. In the **Redirect URI field**, enter the following links . You can enter only one link at a time.

    After you enter a link, click **Configure** and repeat the steps until all of the links are configured.

    a. http://localhost:<port_number>/webclient/VerifyUser.

    b. http://localhost:<port_number>/webclient/grantacces

    c. http://localhost:<port_number>/AADAppGrantSuccess.do

    d. http:/<localhost:<port_number>/AADAuthCode.do

    e. https://identitymanager.manageengine.com/api/public/v1/oauth/redirect

    f. https://demo.m365managerplus.com/oauth/redirect

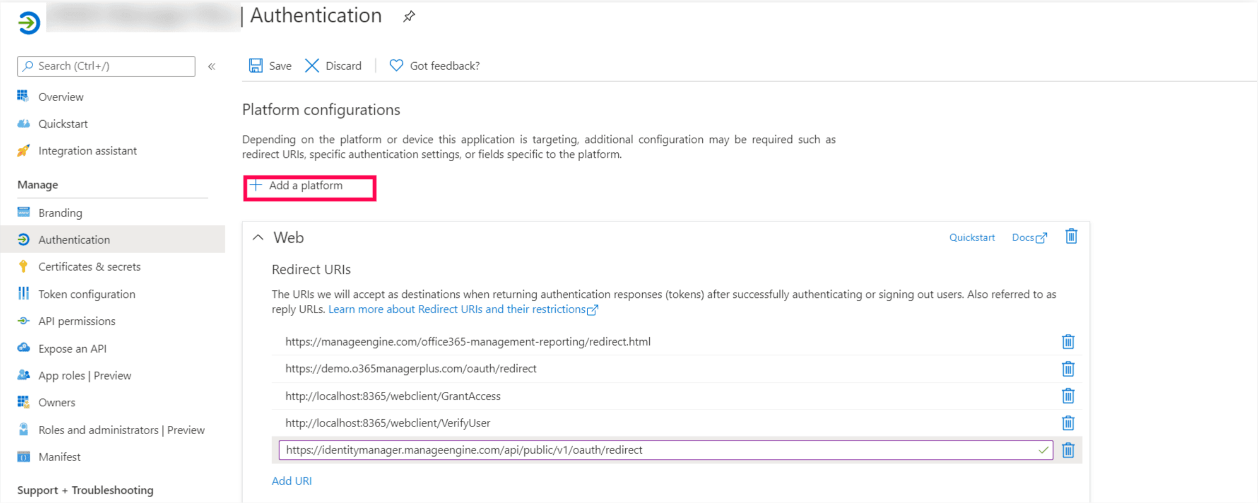
    g. https://manageengine.com/microsoft-365-management-reporting/redirect.html

    where <port_number> refers to the port used by M365 Manager Plus.

Note

- The machine name or IP address can be used in place of <localhost> if the product is configured to use HTTPS. You can configure it by referring to the steps mentioned here. Open **Command Prompt** and enter **ipconfig** to find your machine's IP address.
- Please note that for users with M365 Manger Plus **build 4409 and above**, Redirect URIs **f** and **g** are optional.

13. ou can leave the Logout URL and Implicit grant fields empty. Click **Save.**



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.

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://manageengine.com/office365-management-reporting/redirect.html
https://demo.o365managerplus.com/oauth/redirect
http://localhost:8365/webclient/GrantAccess
http://localhost:8365/webclient/VerifyUser
https://identitymanager.manageengine.com/api/public/v1/oauth/redirect

14. Click **Save.**

15. Click **Manifest** from the left pane.

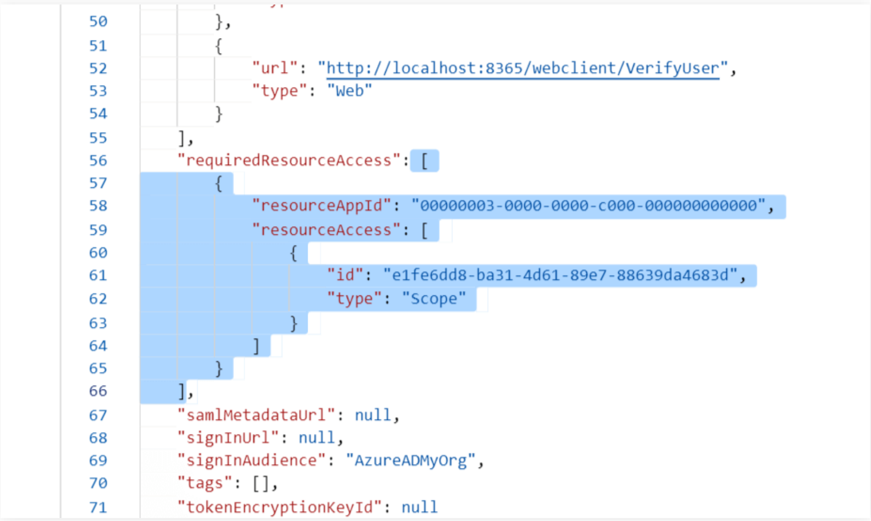
16. Look for *requiredResourceAccess* array in the code.

Copy the entire contents from this file and paste into the section highlighted in the image below.

If you want to modify the permissions, skip this step and follow the steps mentioned in this section.

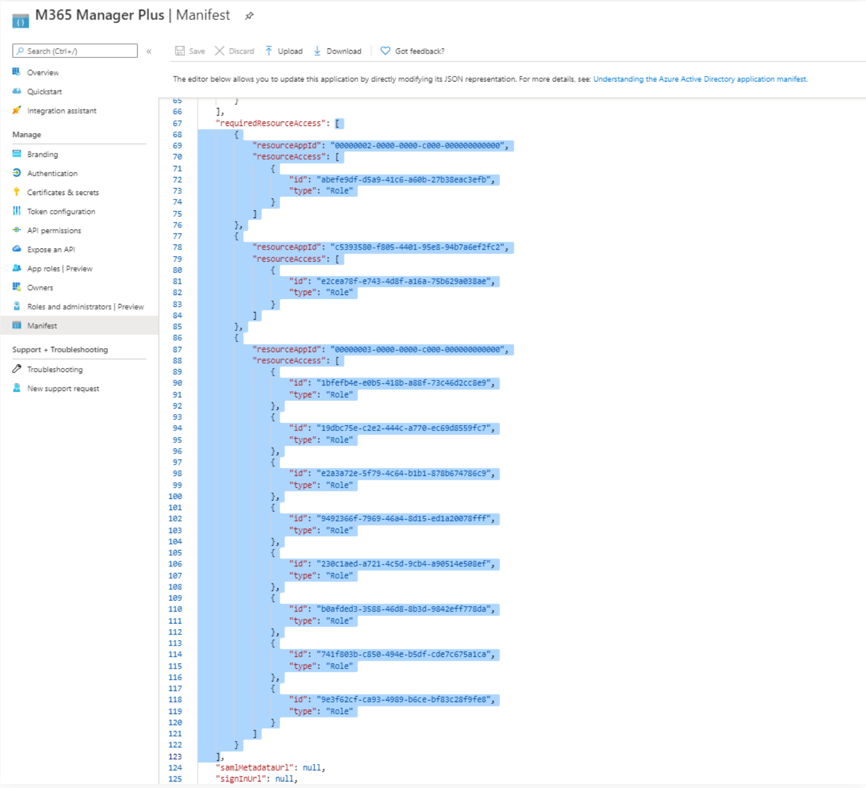
Note:

- If your tenant is being created in **Azure China**, copy the entire contents from this file and paste into the section 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.

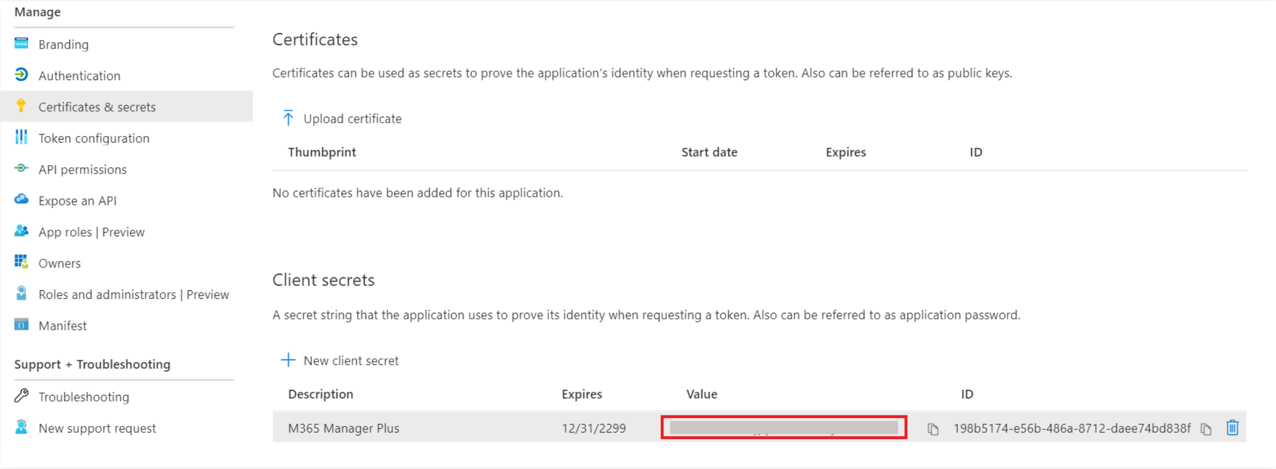


The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
    }
],
"requiredResourceAccess": [
    {
        "resourceAppId": "00000002-0000-0000-c000-000000000000",
        "resourceAccess": [
            {
                "id": "abefe9df-d5a9-41c6-a60b-27b38eac3efb",
                "type": "Role"
            }
        ]
    },
    {
        "resourceAppId": "c5393580-f805-4401-95e8-94b7a6ef2fc2",
        "resourceAccess": [
            {
                "id": "e2cea78f-e743-4d8f-a16a-75b629a038ae",
                "type": "Role"
            }
        ]
    },
    {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
            {
                "id": "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
                "type": "Role"
            },
            {
                "id": "19dbc75e-c2e2-444c-a770-ec69d8559fc7",
                "type": "Role"
            },
            {
                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                "type": "Role"
            },
            {
                "id": "9492366f-7969-46a4-8d15-ed1a20078fff",
                "type": "Role"
            },
            {
                "id": "230c1aed-a721-4c5d-9cb4-a90514e508ef",
                "type": "Role"
            },
            {
                "id": "b0afded3-3588-46d8-8b3d-9842eff778da",
                "type": "Role"
            },
            {
                "id": "741f803b-c850-494e-b5df-cde7c675a1ca",
                "type": "Role"
            },
            {
                "id": "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8",
                "type": "Role"
            }
        ]
    }
],
"samlMetadataUrl": null,
"signInUrl": null,
```

17. Click **Save.**
18. Click **API permissions** from the left pane.
19. In the **Configured permissions** section, click ✔ **Grant admin consent for <your_company_name>.**
20. Click **Yes** in the pop-up that appears.
21. Click **Certificates & secrets** from the left pane.
22. Under the *Client secrets* section, click **New client secret.**
23. 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.
24. Choose when the password should expire.
25. Click **Add.**
26. Copy the string under *Value* and save it. This is the **Application Secret Key,** which you will require later.
27. Go to *Certificates* and click **Upload certificate**. Upload your application certificate as a CER file.
28. If the user has an SSL certificate, the same can be used here. Otherwise, click here for steps to create a self-signed certificate.

Note: Note: Certificate-based authentication is used to contact Microsoft 365 securely and fetch data. During manual configuration, you will be asked to enter your application secret and upload the Application Certificate.



Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

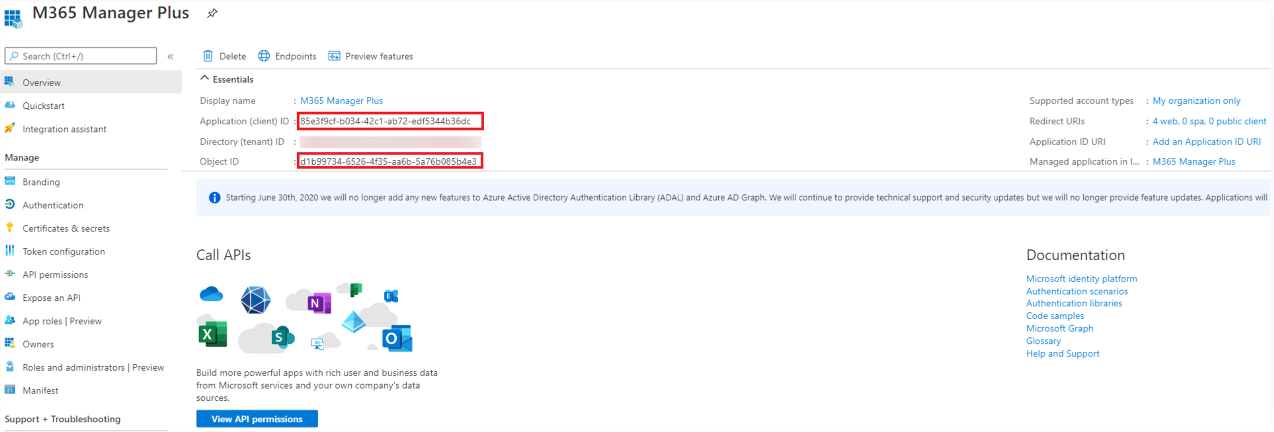
Client secrets

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

Description	Expires	Value	ID
M365 Manager Plus	12/31/2299	[redacted]	198b5174-e56b-486a-8712-daee74bd838f

29. Now go to the **Overview** section in the left pane.

30. 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.



Display name : M365 Manager Plus
Application (client) ID : 85e3f9cf-b034-42c1-ab72-edf5344b36dc
Directory (tenant) ID : [redacted]
Object ID : d1b99734-6526-4f35-aa6b-5a76b085b4e3

Supported account types : My organization only
Redirect URIs : 4 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : M365 Manager Plus

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

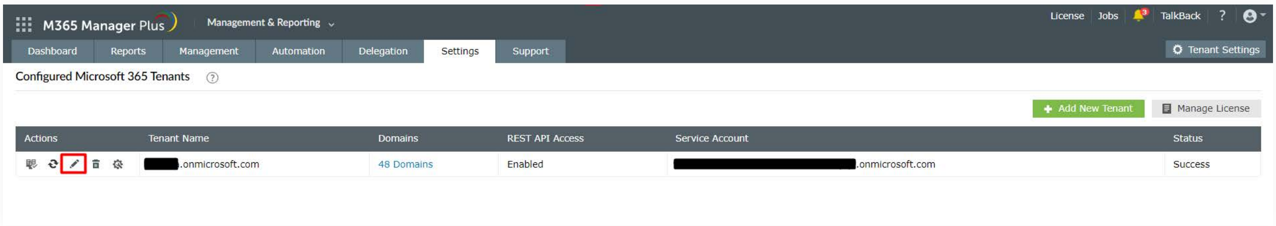
Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
Help and Support

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

Steps to modify a Microsoft 365 tenant

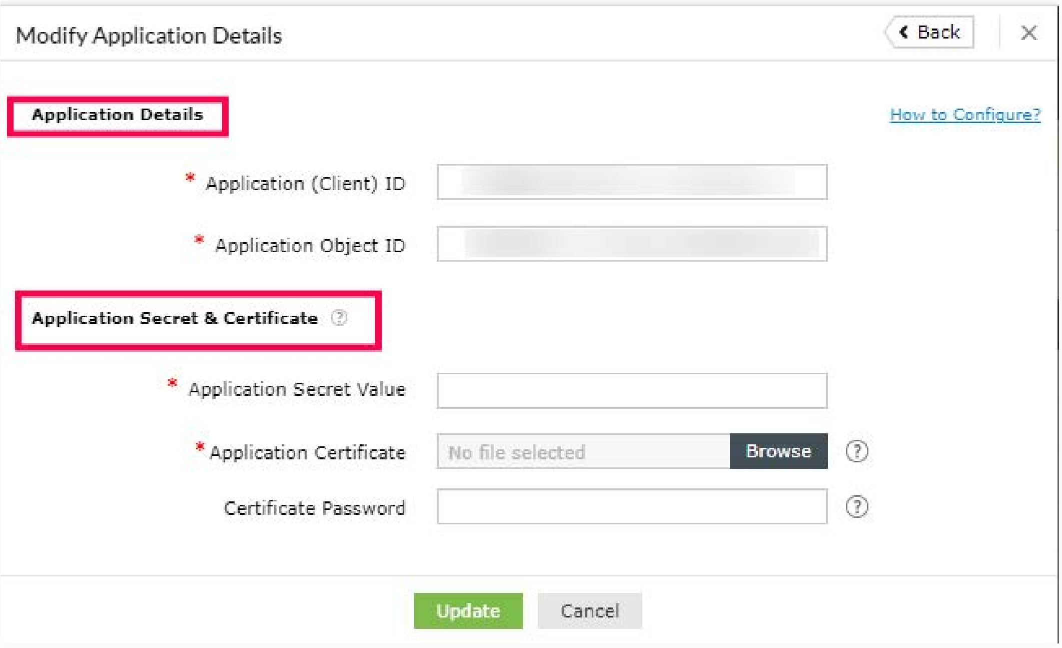
1. Click the **Tenant Settings** option found in the top-right corner.
2. You will see the list of Microsoft 365 tenants configured in M365 Manager Plus.
3. Under the **Actions** column, click the edit icon corresponding to the tenant you need to modify.



Configured Microsoft 365 Tenants

Actions	Tenant Name	Domains	REST API Access	Service Account	Status
	[redacted].onmicrosoft.com	48 Domains	Enabled	[redacted].onmicrosoft.com	Success

4. Click the icon adjacent to **Application Details/Service Account Details** to modify the corresponding values.



Modify Application Details

Application Details

* Application (Client) ID	[redacted]
* Application Object ID	[redacted]

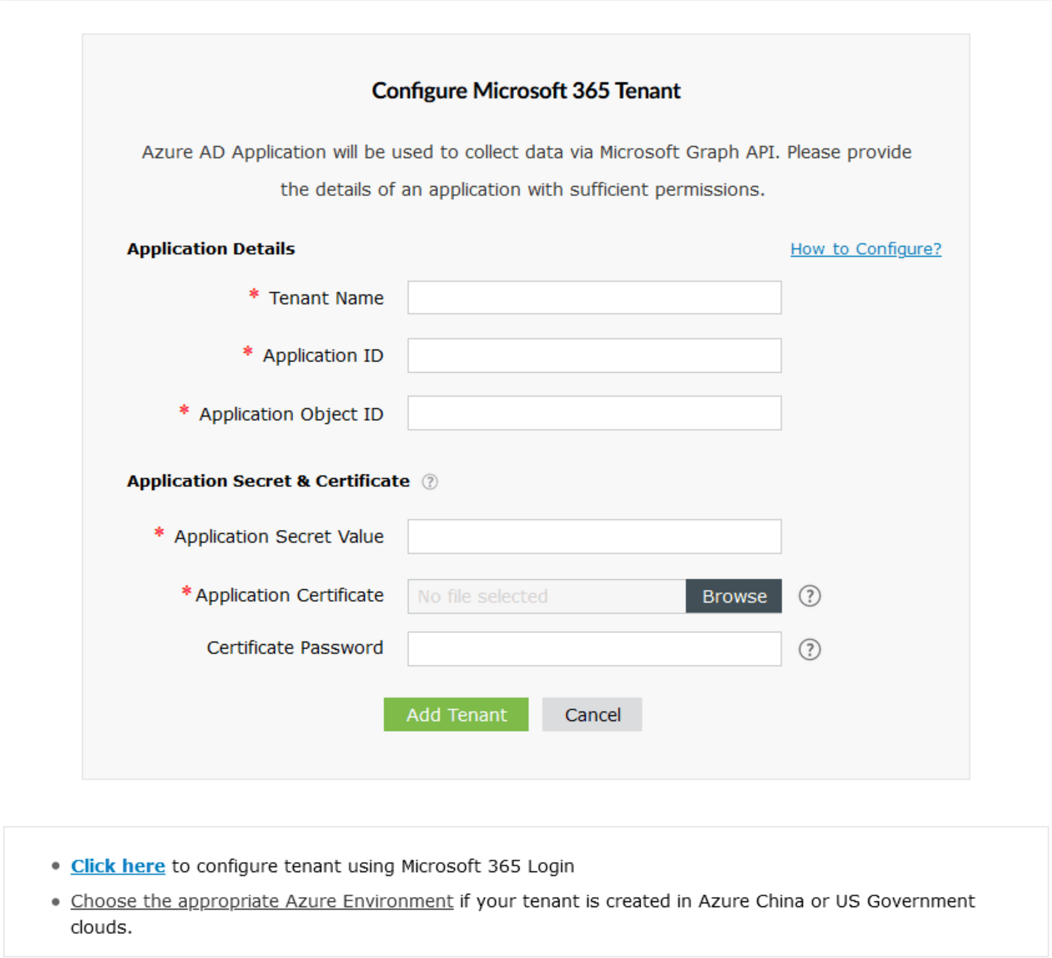
Application Secret & Certificate

* Application Secret Value	
* Application Certificate	No file selected
Certificate Password	

5. Under **Application Details**, you can edit the values in the **Application (Client) ID** and **Application Object ID** fields.
   - You can find these in the application's **Overview** page in the Microsoft Entra admin center.
6. Under **Application Secret &** Certificate, you can modify the **Application Secret Value**, upload the **Application Certificate**, and update the **Certificate Password.**
7. Click **Update** once you have made the changes.

Steps to configure an Entra application in M365 Manager Plus

1. Return to the M365 Manager Plus console where you have the **Configure Microsoft 365 Tenant** pop-up.



Configure Microsoft 365 Tenant

Azure AD Application will be used to collect data via Microsoft Graph API. Please provide the details of an application with sufficient permissions.

Application Details How to Configure?

* Tenant Name

* Application ID

* Application Object ID

Application Secret & Certificate

* Application Secret Value

* Application Certificate: No file selected

Certificate Password

- Click here to configure tenant using Microsoft 365 Login
- Choose the appropriate Azure Environment if your tenant is created in Azure China or US Government clouds.

2. Enter your **Tenant Name**. For example, test.onmicrosoft.com.
3. Paste the **Application ID** and **Application Object ID** values copied in Step 30 into the respective fields.
4. For the **Application Secret Key**, paste the value copied in Step 26 from the Manual Microsoft 365 tenant configuration section.
5. Upload a PFX file of the certificate that has been uploaded in the Azure portal. Refer to Step 27 in the Steps to create an Entra application section.
6. Enter your certificate password.
7. If you have an SSL certificate, you can upload the same in the appropriate field.
8. Click **Add Tenant.**
9. You should now see that REST API access is enabled for the account you configured.

Steps to create a self-signed certificate

1. Run the following command in Windows PowerShell as an administrator:

   Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force -Scope process

2. Go to the *<Installation Directory>\bin* folder and run the **Create-selfsignedcertificate.ps1** script as an administrator.
3. While running the script, you will be asked to add a common name for the certificate, start and end date (yyyy-MM-dd) for the certificate's validity, and a private key to protect it.
4. Once you enter the values, the script will create a PFX file (contains both public and private key) in the *bin* folder.
5. The PFX file needs to be uploaded in M365 Manager Plus, while the CER file should be uploaded in the Azure portal of your application.

Appendix

Minimum scope

Roles required for an Entra application

The roles required by an Entra application configured for M365 Manager Plus are listed below.

Table 3: Roles required by the configured Entra application.

Role Name	Scope
Privileged Authentication Administrator	Create, manage, and delete users and their authentication methods.
Helpdesk Administrator	Change passwords, invalidate refresh tokens, and monitor service health.
Exchange Administrator	Create, manage, and delete Exchange Online mailboxes.

Permissions required for an Entra application

The permissions required by an Entra application configured for M365 Manager Plus are listed below.

Table 4: Roles and permissions required by the Entra application.

Module	API Name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	User creation, modification, deletion and restoration.
		Group.ReadWrite.All	Group creation, modification, deletion, restoration, add or remove members and owners.

		AdminsitrativeUnit.ReadWrite.All	Add members to administrative units.
		RoleManagement.ReadWrite.Directory	Add directory roles to users.
		UserAuthenticationMethod.ReadWrite.All	Allows the application to read and write authentication methods of all users
		Policy.ReadWrite.AuthenticationMethod	Allows the application to change the MFA status of all users and configure their default MFA method.
	Exchange Online	Exchange.ManageAsApp	Used to execute Exchange Online PowerShell cmdlets via the configured Entra application
	SharePoint Online	Sites.Manage.All	Allow the app to read, create, update, and delete document libraries and lists in all site collections.
Reporting	Microsoft Graph	User.Read.All	Get user and group member reports.
		Group.Read.All	Get 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.
		ChannelMember.Read.All	Get Microsoft Teams channel member reports.
		Application.Read.All	Get Entra application details.
		Sites.Read.All	Get details on SharePoint sites.
		Policy.Read.All	Configure conditional access policy details.
		Calendars.Read	Get users' calendar details.

		ReportSettings.Read.All	Enables the configured Entra application to retrieve tenant-level settings from the tenant where it is configured.
	Office 365 Management	ActivityFeed.Read	Read the audit data for the organization.
	Exchange Online	Exchange.ManageAsApp	Used to execute Exchange Online PowerShell cmdlets via the configured Entra application
	SharePoint Online	Sites.Read.All	Allow the app to read documents and list items in all site collections.
Auditing and alerting	Office 365 Management	ActivityFeed.Read	Read the activity data for the organization.
	Exchange Online	Exchange.ManageAsApp	Used to execute Exchange Online PowerShell cmdlets via the configured Entra application
	SharePoint Online	InformationProtectionPolicy.Read.All (not available in Azure China tenants)	Get data on published sensitivity labels used in the tenant.
Monitoring	Microsoft Graph	ServiceHealth.Read.All	Get health and performance reports.
Content search	Microsoft Graph	Mail.Read	Get content search reports.
Configuration	Microsoft Graph	Application.ReadWrite.All	Modify the application details.
Backup	Office 365 Exchange Online	full_access_as_app	Use Exchange Web Services to back up and restore mailboxes.

ManageEngine
M365 Manager Plus

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About M365 Manager Plus

ManageEngine M365 Manager Plus is an one-stop solution for Microsoft 365 management, reporting, auditing and monitoring that helps simplify Microsoft 365 governance, administration, and security. M365 Manager Plus enables admins to gain visibility into various Microsoft 365 components and display key insights through more than 700 out-of-the-box reports. It eliminates the need for writing complex PowerShell scripts and reduces costs associated with administering Microsoft 365.

For more information about M365 Manager Plus, visit www.m365managerplus.com.

$ Get Quote

⤓ Download