

ManageEngine  
M365 Manager Plus

# Microsoft 365 Tenant Configuration

[www.microsoft365managerplus.com](http://www.microsoft365managerplus.com)

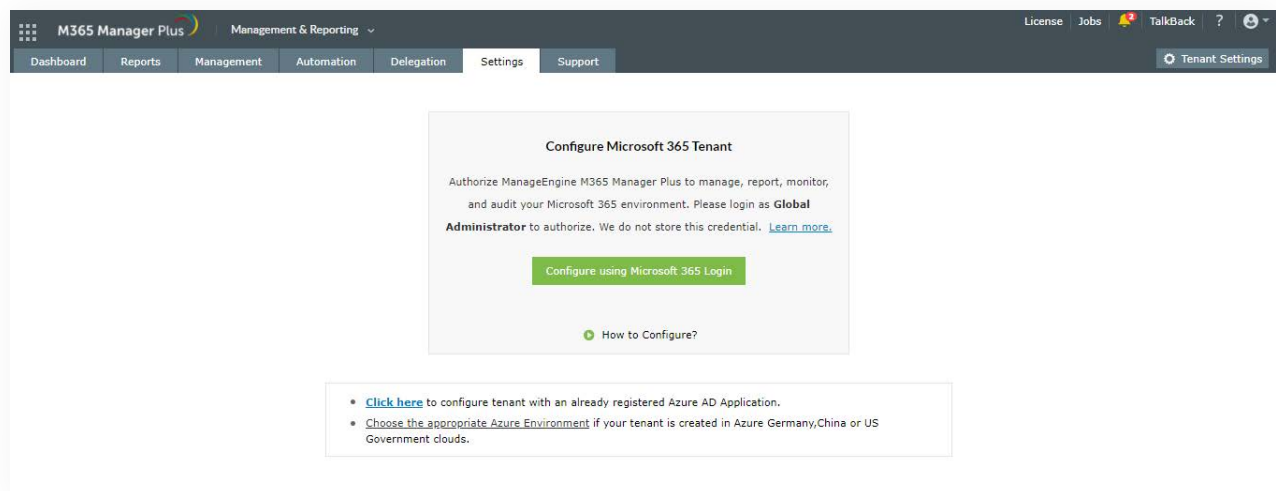
## Table of Contents

<b>Automatic Microsoft 365 tenant configuration</b>	<b>1</b>
<b>Steps to modify REST API permissions</b>	<b>3</b>
<b>Manual Microsoft 365 tenant configuration</b>	<b>5</b>
Steps to create an Azure AD application	6
<b>Steps to modify a Microsoft 365 tenant</b>	<b>10</b>
Steps to configure an Azure application in M365 Manager Plus	11
Steps to configure a service account in M365 Manager Plus	12
Steps to create a self-signed certificate	12
<b>How to configure an MFA-enabled service account</b>	<b>12</b>
Steps to configure Trusted IPs	13
Steps to configure Conditional Access	13
<b>Appendix</b>	<b>14</b>
Minimum scope	14

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

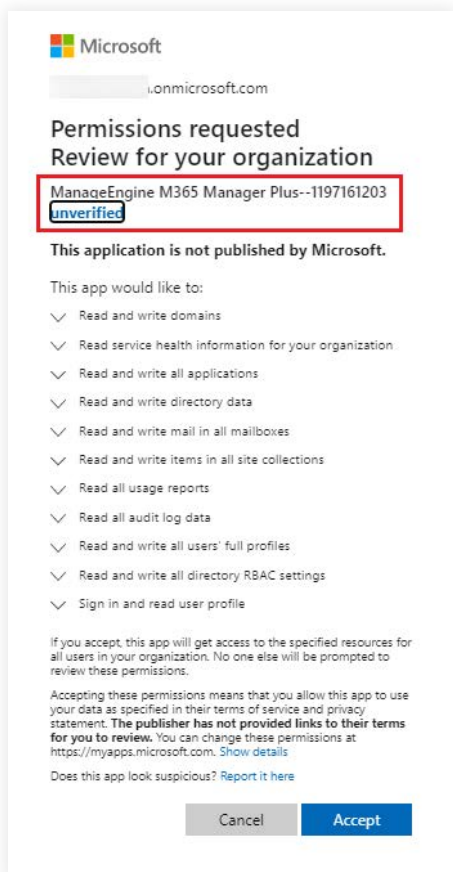
1. Log in to M365 Manager Plus as an administrator. The default username and password are *admin* and *admin* respectively.
2. Choose the **Tenant Settings** option found in the top-right corner.
3. If you are configuring your first tenant, click **Configure using Microsoft 365 Login**. Otherwise, choose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



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.

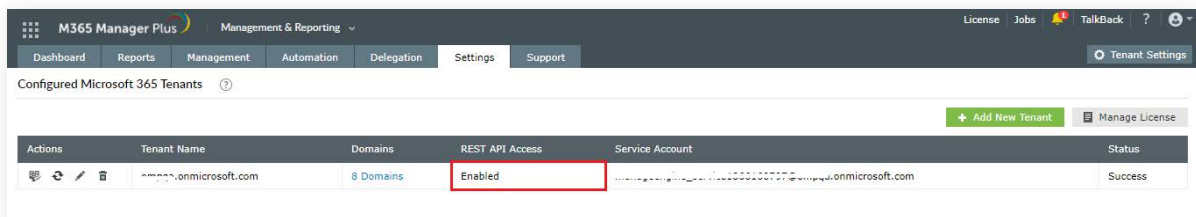


8. Go through the list of permissions and click **Accept**.

**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](#).

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

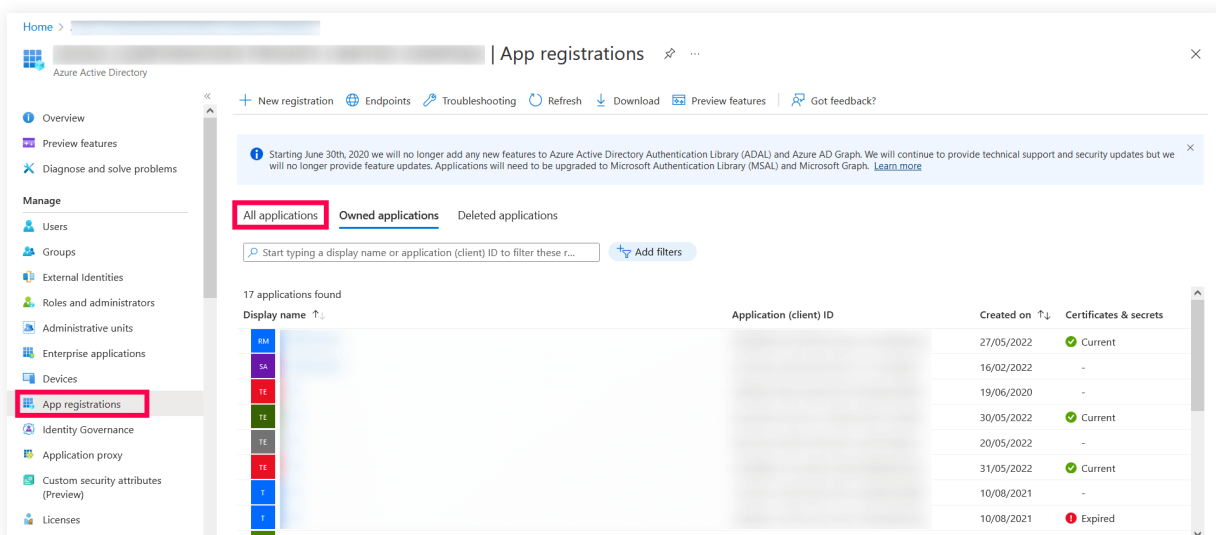
Though we suggest providing all the [recommended permissions](#), organizational policies may not allow this.

In this section, you will learn how to modify the REST API permissions for an already configured tenant.

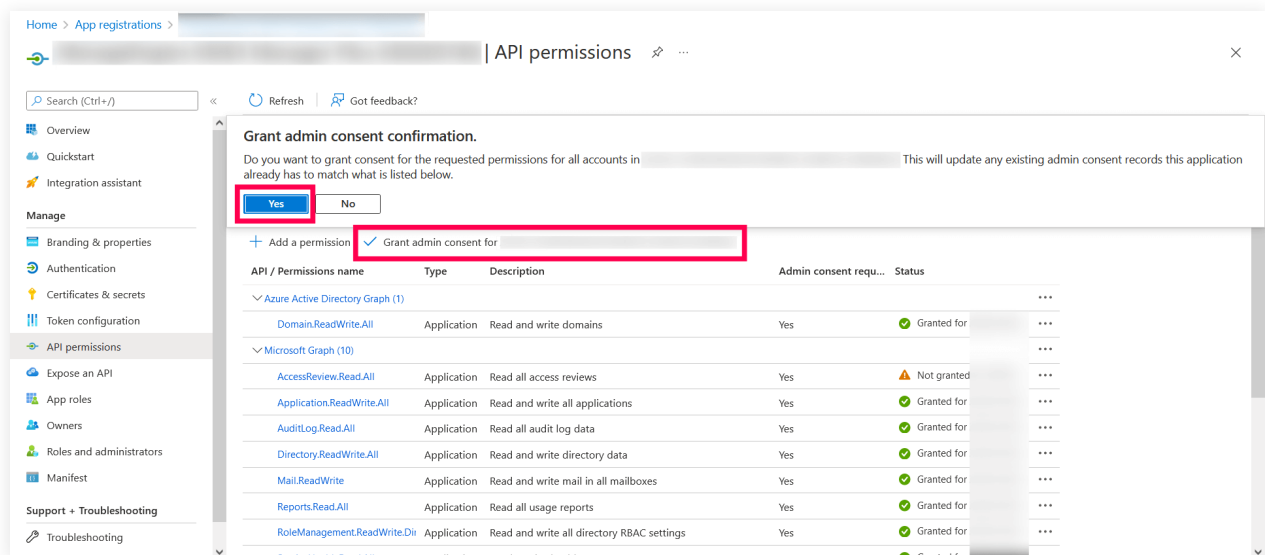
If you are looking for a way to configure a tenant with only the permissions required for the features you want to use, [here](#) are the steps to do that manually.

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

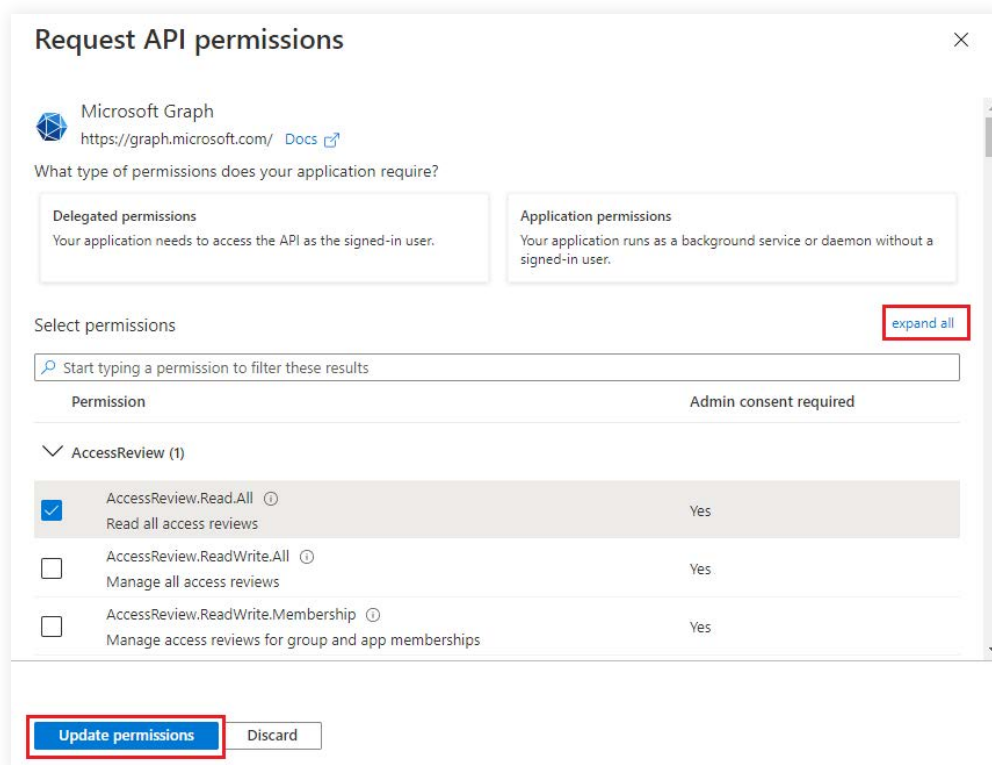
1. Log in to the [Azure AD admin center](#).
2. Click Azure **Active Directory** from the left pane.
3. Choose **App registration** under Manage.
4. Select **All applications**.



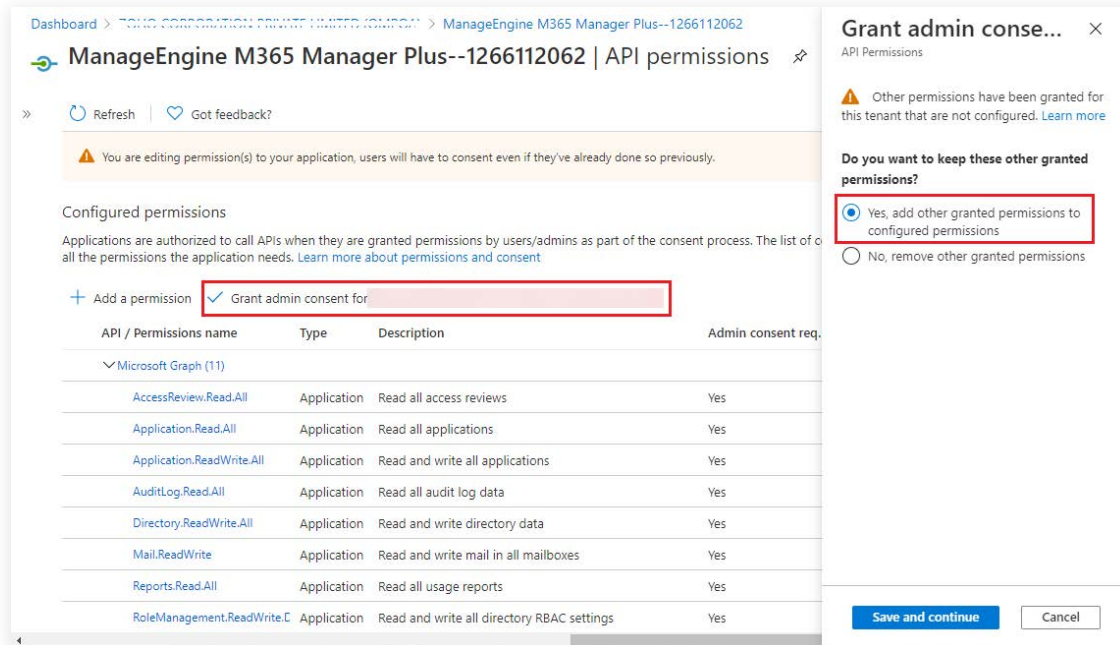
5. Search for the application name you noted earlier (see step 7) and click it.
6. Under *Manage*, select **API Permissions**.
7. Choose **Microsoft Graph**.



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

**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](#)

### 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.

[How to Configure?](#)

**Application Details**

\* Tenant Name

\* Application ID

\* Application Object ID

**Application Secret & Certificate** ?

\* Application Secret Key

\* Application Certificate   ?

Upload PFX certificate(.pfx) file

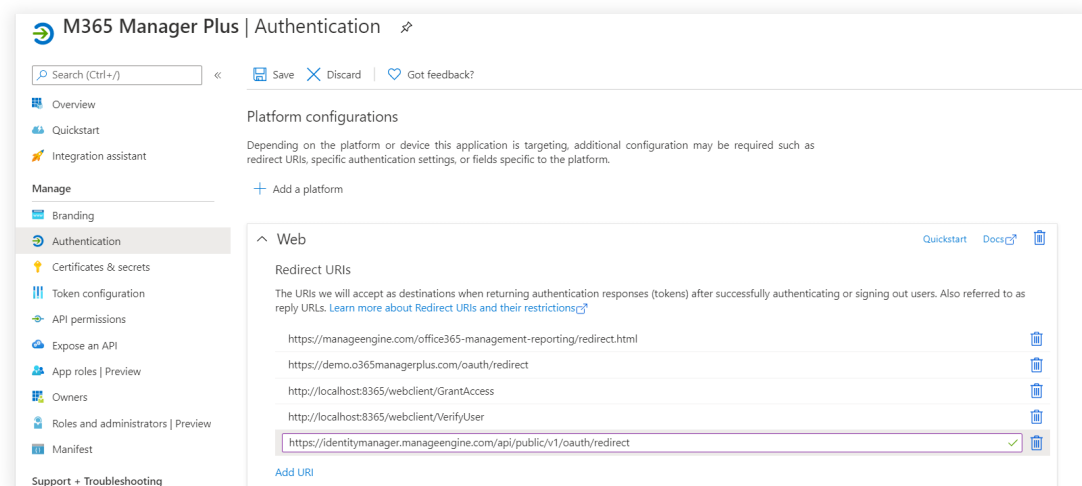
- [Click here](#) to configure tenant using Microsoft 365 Login
- [Choose the appropriate Azure Environment](#) if your tenant is created in Azure Germany,China or US Government clouds.

## 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, under *Web applications*, click **Web**.
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](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. Similarly, using the Add URI option add [http://localhost:port\\_number/AADAppGrantSuccess.do](http://localhost:port_number/AADAppGrantSuccess.do) and [http://localhost:port\\_number/AADAuthCode.do](http://localhost:port_number/AADAuthCode.do) as URIs as well.
18. Click **Add URI** again to add the below Redirect URIs in the subsequent rows. Please note that for users with M365 Manger Plus **build 4409 and above**, 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. The 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 press the **Enter** key.

You can find your IPv4 address in the results shown.

19. Click **Save**.
20. Click **Manifest** from the left pane.
21. Look for *requiredResourceAccess* array in the code.
22. 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 Germany**, copy the entire contents from [this file](#) and paste into the section highlighted in the image below.
- 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.

```

50     },
51     {
52         "url": "http://localhost:8365/webclient/VerifyUser",
53         "type": "Web"
54     }
55 ],
56 "requiredResourceAccess": [
57     {
58         "resourceAppId": "00000003-0000-0000-c000-000000000000",
59         "resourceAccess": [
60             {
61                 "id": "e1fe6dd8-ba31-4d61-89e7-88639da4683d",
62                 "type": "Scope"
63             }
64         ]
65     }
66 ],
67 "samlMetadataUrl": null,
68 "signInUrl": null,
69 "signInAudience": "AzureADMyOrg",
70 "tags": [],
71 "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.

```

65     },
66     {
67         "requiredResourceAccess": [
68             {
69                 "resourceAppId": "00000003-0000-0000-c000-000000000000",
70                 "resourceAccess": [
71                     {
72                         "id": "abef9df-d5a9-41c6-8680-270388a3c8fd",
73                         "type": "Role"
74                     }
75                 ]
76             }
77         ]
78     },
79     {
80         "resourceAppId": "c393580-f805-44a1-95e8-940786f2fca2",
81         "resourceAccess": [
82             {
83                 "id": "c0c075f-6743-46df-a16a-7506298030e",
84                 "type": "Role"
85             }
86         ]
87     },
88     {
89         "resourceAppId": "00000003-0000-0000-c000-000000000000",
90         "resourceAccess": [
91             {
92                 "id": "1bfe04e-e805-418b-888f-73c46d2cc8e9",
93                 "type": "Role"
94             },
95             {
96                 "id": "192bc75e-c2e2-444c-8770-ec69d8559fc7",
97                 "type": "Role"
98             },
99             {
100                "id": "c0c075f-6743-46df-a16a-7506298030e",
101                "type": "Role"
102            },
103             {
104                "id": "9492366f-7969-4694-8d15-ed1a2b078fff",
105                "type": "Role"
106            },
107             {
108                "id": "238c1aed-8721-4c5d-9c04-8905144588ef",
109                "type": "Role"
110            },
111             {
112                "id": "0ea4de03-3588-46d8-8b3d-9842ef778da",
113                "type": "Role"
114            },
115             {
116                "id": "741f08bb-c850-494e-b5df-cd67c7591ca",
117                "type": "Role"
118            },
119             {
120                "id": "8a3fe2cf-ca93-4989-bc0c-bf93c28f9fe8",
121                "type": "Role"
122            }
123         ]
124     },
125     "samlMetadataUrl": null,
126     "signInUrl": null,

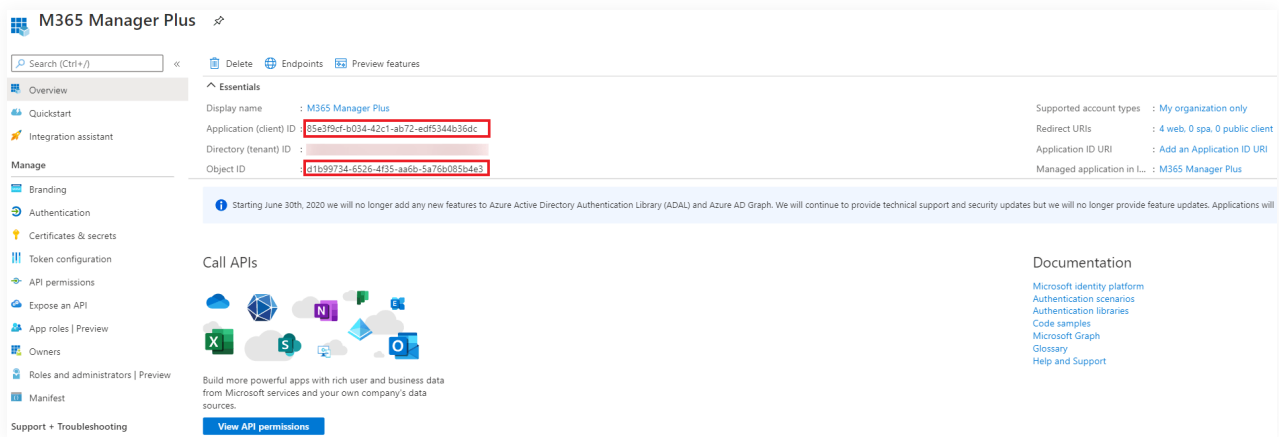
```

23. Click **Save**.
24. Click **API permissions** from the left pane.
25. In the **Configured permissions** section, click **✓ Grant admin consent for <your\_company\_name>**.
26. Click **Yes** in the pop-up that appears.
27. Click **Certificates & secrets** from the left pane.
28. Under the *Client secrets* section, click **New client secret**.
29. 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.
30. Choose when the password should expire.
31. Click **Add**.
32. Copy the string under *Value* and save it. This is the **Application Secret Key**, which you will require later.
33. Go to *Certificates* and click **Upload certificate**. Upload your application certificate as a CER file.
34. 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.


The screenshot shows the 'Manage' section of the M365 Manager Plus interface. The left sidebar contains navigation options: Branding, Authentication, Certificates & secrets (selected), Token configuration, API permissions, Expose an API, App roles | Preview, Owners, Roles and administrators | Preview, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main content area is divided into two sections: 'Certificates' and 'Client secrets'. The 'Certificates' section has an 'Upload certificate' button and a table with columns 'Thumbprint', 'Start date', 'Expires', and 'ID'. Below this, it states 'No certificates have been added for this application.' The 'Client secrets' section has a '+ New client secret' button and a table with columns 'Description', 'Expires', 'Value', and 'ID'. The table contains one entry for 'M365 Manager Plus' with an expiration date of '12/31/2299' and a value field that is highlighted with a red box. The ID for this entry is '198b5174-e56b-486a-8712-dae74bd838f'.

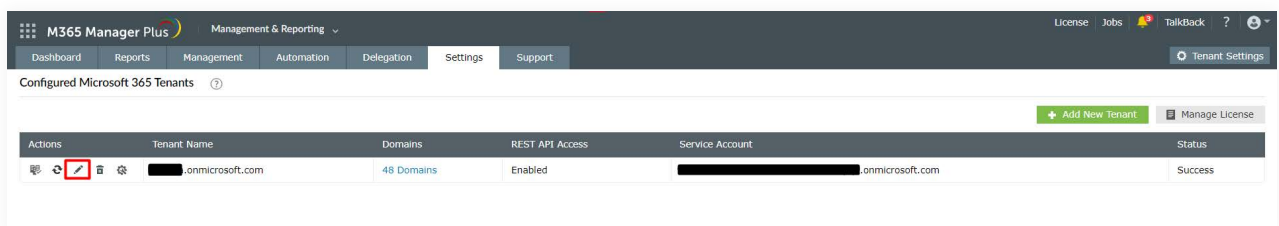
32. Now go to the **Overview** section in the left pane.
33. Copy the **Application (client) ID** and **Object ID** values and save them. You will need these values to configure your tenant in the M365 Manager Plus portal.




34. Refer to [this table](#) to learn about the roles that must be assigned to the application.

## Steps to 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.



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

**Modify Application Details** ← Back | ✕

**Application Details** [How to Configure?](#)

\* Application (Client) ID

\* Application Object ID

**Application Secret & Certificate** ?

\* Application Secret Value

\* Application Certificate   ?

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 [Azure AD 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 Azure 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**

\* Tenant Name

\* Application ID

\* Application Object ID

**Application Secret & Certificate** ?

\* Application Secret Key

\* Application Certificate   ?

Upload PFX certificate(.pfx) file

[How to Configure?](#)

- [Click here](#) to configure tenant using Microsoft 365 Login
- [Choose the appropriate Azure Environment](#) if your tenant is created in Azure Germany,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 34 into the respective fields.
4. For the **Application Secret Key**, paste the value copied in Step 32 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 34 in the Steps to create an Azure AD 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 configure a service account in M365 Manager Plus

1. Now the service account must be configured. To do this, click the **edit** option under the **Actions** column.
2. Click 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 **Update**, and close the pop-up window.

**Note:** If your service account is MFA-enabled, please check [this section](#).

## 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.

## 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 or Trusted IPs, you need an **Azure AD Premium P1** license.

## Steps to configure Trusted IPs

- Log in to [portal.azure.com](https://portal.azure.com) using your Global Administrator credentials.
- Under *Azure services*, click **Azure Active Directory**.
- Choose **Security** from the left pane.
- Under the *Manage* category in the left pane, click **MFA**.
- 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 **Save**.

## 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.

- Log in to [portal.azure.com](https://portal.azure.com) using your Global Administrator credentials.
- Under *Azure services*, click **Azure Active Directory**.
- Choose Security from the left pane.
- Under the *Protect* category in the left pane, click **Conditional Access**.
- Click **New Policy**.
- The drop-down list contains options to either **Create new policy** or **Create new policy from templates (preview)**. Click on **Create new policy** to continue.
- Provide a name for the policy.
- Under **Assignments**, choose **Users or workload identities**.
- Click the **Users and groups** option.
- Click the **Exclude** tab and select the **Users and groups** check box.
- Choose the M365 Manager Plus users for whom MFA should not be enforced.
- Click **Select**.
- Under the *Access controls* section, click **Grant**.
- Select the **Grant access** radio button and the **Require multi-factor authentication** check box.
- Click **Select**.
- Click **Create**.

## 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
<b>Management</b>	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
<b>Reporting</b>	Global Reader	Get reports on all Microsoft 365 services
	Security Reader	Get audit logs and mailbox reports.
<b>Auditing and Alerting</b>	Security Reader	Get audit logs and sign-in reports
<b>Monitoring</b>	-	-
<b>Content Search</b>	-	-

**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.
- If the Exchange Administrator role is not provided, add the service account to the role group with View-Only Audit Logs role. This role is required for audit and audit-based reports. To learn how to set up this account, click [here](#).

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.
		AdministrativeUnit.ReadWrite.All	Add members to administrative units.
		RoleManagement.ReadWrite.Directory	Add directory roles to users.
	SharePoint	Sites.FullControl.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	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 (not available in Chinese tenant)	Get Microsoft Teams channel members report.
		Application.Read.All	Get Azure AD application details.
		Sites.Read.All	Get SharePoint sites details.
	Policy.Read.All	Configure conditional access policies details.	
	Calendars.Read	Get users' calendar details.	
	SharePoint	Sites.Read.All	Allow the app to read documents and list items in all site collections.
	Office 365 Management	ActivityFeed.Read	Read the audit data for organization.

<b>Auditing and Alerting</b>	Office 365 Management	ActivityFeed.Read	Get audit reports and alerts.
<b>Monitoring</b>	Microsoft Graph	ServiceHealth.Read.All	Get health and performance reports.
<b>Content Search</b>	Microsoft Graph	Mail.Read	Get content search reports.
<b>Configuration</b>	Microsoft Graph	Application. ReadWrite.All	Modify the application details.
<b>Backup</b>	Office 365 Exchange Online	full_access_as_app	Use Exchange Web Services to back up and restore mailboxes.

## Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus  
Exchange Reporter Plus | RecoveryManager Plus

## About M365 Manager Plus

ManageEngine M365 Manager Plus is a web-based, one-stop solution for Microsoft 365 management, auditing and reporting that helps simplify management, ensure security and compliance and gain valuable insights on all the different components of Microsoft 365. 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 [manageengine.com/microsoft-365-management-reporting/](https://manageengine.com/microsoft-365-management-reporting/).

\$ Get Quote

↓ Download