

# **Microsoft 365 tenant configuration in ADManager Plus**

Organizations deploy Microsoft 365 to ensure continuous availability of resources to their employees and enhance their productivity. However, managing this cloud-based environment can be quite a challenge. ManageEngine ADManager Plus alleviates the Microsoft 365 administrative burden by letting you create user accounts in single and bulk, and set and manage necessary licenses. It also enables the effortless generation of Microsoft 365 reports.

Given below are the prerequisites—hardware and software requirements essential for ensuring a trouble free ADManager Plus—Microsoft 365 integration.

## System requirement

### Essential hardware

Hardware	Minimum	Recommended
Processor	2.4 GHz	3 GHz
Number of cores	4	6 or more
RAM	8 GB	16 GB
Disk space	200 GB (SSD preferred)	500 GB (SSD preferred)
Disk throughput	5 MB/s	20 MB/s

### Supported platforms

The following Microsoft Windows operating system versions are supported:

Windows Server 2022	Windows 11
Windows Server 2019	Windows 10
Windows Server 2016	Windows 8.1
Windows Server 2012 R2	Windows 8
Windows Server 2012	Windows 7
Windows Server 2008 R2	Windows Vista
Windows Server 2008	Windows XP

### Supported browsers

The application works seamlessly with the latest version of modern browsers. It requires one of the following browsers to be installed in the system for working with the client:

- Internet Explore 9.0 and above
- Mozilla Firefox 45.0 and above
- Google Chrome 45.0 and above
- Microsoft Edge

\*we recommend using the latest version of the browser for better security and best possible experience.

## Prerequisites for Microsoft 365 Integration

Ensure the installation of the below-listed modules:

**1. Microsoft .NET framework 4.8 or later**

Refer this [link](#) to determine the version of .NET framework installed on your computer. You can download .NET framework 4 from [here](#).

**2. Windows PowerShell 5.1**

To determine the version of PowerShell installed, run the command `$PSVersionTable` from Windows PowerShell. If the version is below 5.1 or if PowerShell is not installed download from [here](#).

**3. MSOnline PowerShell for Azure Active Directory[(V1) 1.1.166.0]**

Run the PowerShell Cmdlet `Import-Module MSOnline` from Windows PowerShell to determine whether this module is installed. The PowerShell Cmdlet returns an error if the module is not installed and there will be no message to be displayed if the module is already installed. To install the module, open PowerShell as an administrator and enter the following cmdlet: *Install-Module -Name MSOnline -RequiredVersion 1.1.166.0 -Force*.

**4. Administrative privileges**

The account must have global administrator (preferred) or user management administrator privilege in Microsoft 365.

**5. Other requirements**

- Make sure your firewall settings allow access to these domains.
- The 64-bit version of the product must be installed.

## Steps for automatic Microsoft 365 tenant configuration in ADManager Plus

1. Navigate to **Domain/Tenant Settings > Microsoft 365** tab.
2. Click on **+Add New Tenant**.
3. Click **Configure using Microsoft 365 Login** button.
4. Select the required AD domains which are to be linked with this account. It is essential to link the on-premises domains with Microsoft 365 domains as it is needed to apply OU-based restrictions.
5. Click **Proceed** in the dialog box that appears. You will be redirected to the Microsoft 365 login page where you will be required to login with the Global Administrator's credentials.
6. The Microsoft 365 login portal will list the permissions requested for your organization. Once you are informed of these permissions, click **Accept**.
7. Once the tenant configuration is successful, it will be listed in the Microsoft365 window.

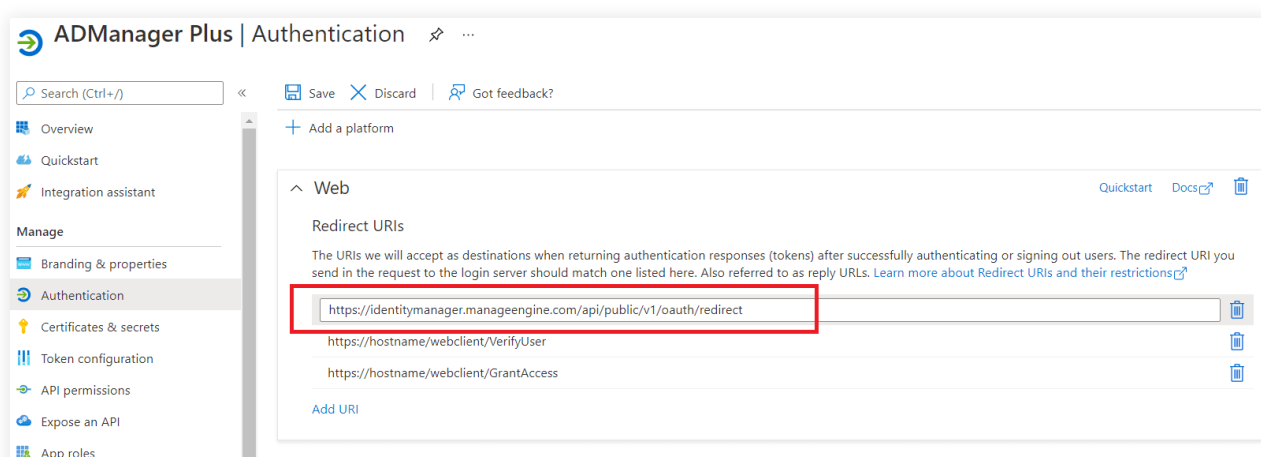
**Note:** If the automatic configuration fails due to permission issues, the tenant must be configured manually.

## Steps to manually configure Microsoft 365 tenant

**Prerequisite:** A service user account with at least View-Only Organization Management, View-Only Audit Logs, and Service Administrator permissions.

### 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 ADManager 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:8080/webclient/VerifyUser** or **https://192.345.679.345:8080/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:8080/webclient/GrantAccess** or **https://192.345.679.345:8080/webclient/GrantAccess**.
17. Similarly, using the Add URI option add **http://localhost:port\_number/AADAppGrantSuccess.do** and **http://localhost:port\_number/AADAuthCode.do** as URIs as well.
18. Again click **Add URI** to add the below REDIRECT URIs in the subsequent rows. Please note that for **users with ADManger Plus build 7200 or higher, REDIRECT URIs (b) and (c) are optional**.
  - <https://identitymanager.manageengine.com/api/public/v1/oauth/redirect>
  - <https://demo.o365managerplus.com/oauth/redirect>
  - <https://manageengine.com/microsoft-365-management-reporting/redirect.html>



**Note:**

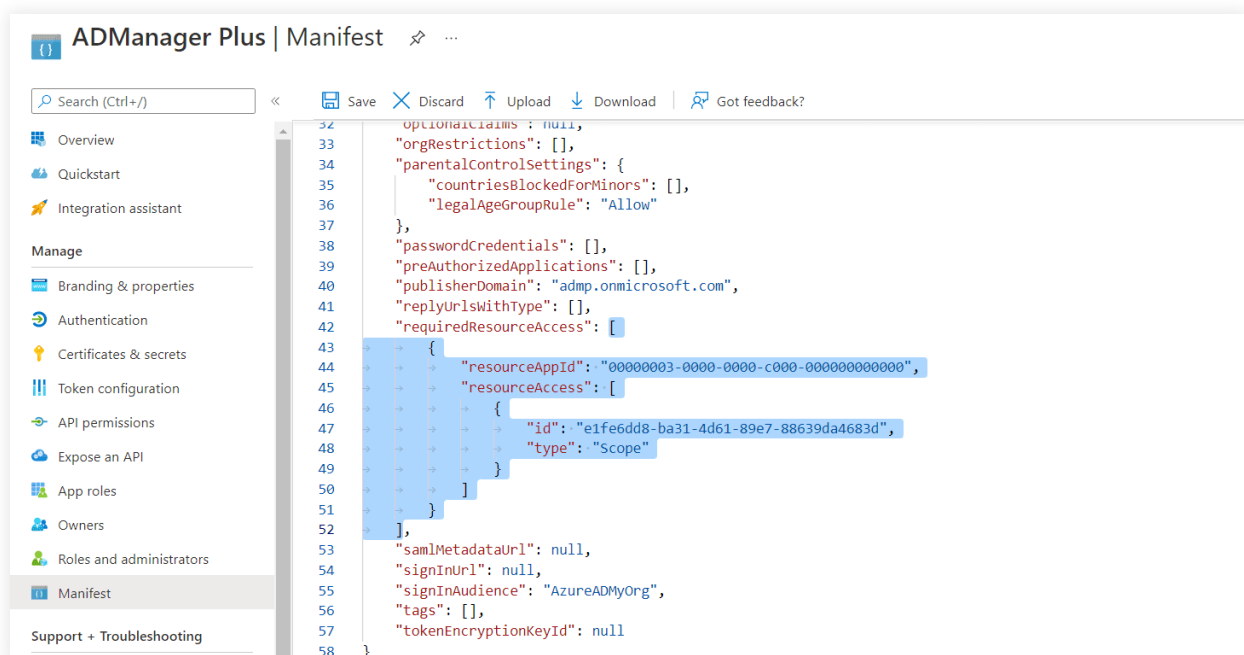
1. The REDIRECT URI must adhere to the following:
  - It must be fewer than 256 characters in length.
  - It should not contain wildcard characters.
  - It should not contain query strings.
  - It must start with HTTPS or http://localhost.
  - It must be a valid and unique URL.
  - For HTTP, the URI value is: http://localhost:8080. If HTTP is used, the machine name or IP address cannot be used in the place of localhost.
  - For HTTPS, the URI value is: https://192.345.679.345:8080 or https://testmachine:8080 (where <testmachine> is the hostname of the machine where ADManager Plus is installed).
2. The REDIRECT URI format varies according to the connection type (HTTP/HTTPS) that has been configured in ADManager Plus.
3. 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.

19. Click **Save**.

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

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

22. Copy the contents of [this file](#) and paste the content as highlighted in the image below, then click **Save**. If you want to modify the permissions to be provided, skip this step and follow the steps mentioned in [this guide](#).



### 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 content in the file, it should look like the image below.

The screenshot shows the ADManager Plus Manifest editor interface. The left sidebar contains a navigation menu with sections: Overview, Quickstart, Integration assistant, Manage, and Support + Troubleshooting. The 'Manage' section is expanded, showing options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The 'Manifest' option is selected. The main area displays a JSON configuration for roles and resource access. The configuration includes a list of roles with their IDs and types, and a list of resource access entries with their IDs and types. The roles are listed under 'parentalControlSettings' and 'passwordCredentials'. The resource access entries are listed under 'resourceAccess'.

```

34 "parentalControlSettings": {
35   "countriesBlockedForMinors": [],
36   "legalAgeGroupRule": "Allow"
37 },
38 "passwordCredentials": [],
39 "preAuthorizedApplications": [],
40 "publisherDomain": "admpmsdn.onmicrosoft.com",
41 "replyUrlsWithType": [],
42 "requiredResourceAccess": [
43   {
44     "resourceAppId": "00000003-0000-0000-c000-000000000000",
45     "resourceAccess": [
46       {
47         "id": "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
48         "type": "Role"
49       },
50       {
51         "id": "19dbc75e-c2e2-444c-a770-ec69d8559fc7",
52         "type": "Role"
53       },
54       {
55         "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
56         "type": "Role"
57       },
58       {
59         "id": "9492366f-7969-46a4-8d15-ed1a20078fff",
60         "type": "Role"
61       },
62       {
63         "id": "230c1aed-a721-4c5d-9cb4-a90514e508ef",
64         "type": "Role"
65       },
66       {
67         "id": "b0afded3-3588-46d8-8b3d-9842eff778da",
68         "type": "Role"
69       },
70       {
71         "id": "741f803b-c850-494e-b5df-cde7c675a1ca",
72         "type": "Role"
73       },
74       {
75         "id": "9e3f62cf-ca93-4989-b6ce-bf83c28f9fe8",
76         "type": "Role"
77       },
78       {
79         "id": "79c261e0-fe76-4144-aad5-bdc68fbc4037",
80         "type": "Role"
81       },
82       {
83         "id": "246dd0d5-5bd0-4def-940b-0421030a5b68",
84         "type": "Role"
85       },
86       {
87         "id": "798ee544-9d2d-430c-a058-570e29e34338",
88         "type": "Role"
89       }
90     ]
91   },
92   {
93     "resourceAppId": "c5393580-f805-4401-95e8-94b7a6ef2fc2",
94     "resourceAccess": [
95       {
96         "id": "e2cea78f-e743-4d8f-a16a-75b629a038ae",
97         "type": "Role"
98       }
99     ]
100   },
101   {
102     "resourceAppId": "00000002-0000-0000-c000-000000000000",
103     "resourceAccess": [
104       {
105         "id": "abefe9df-d5a9-41c6-a60b-27b38eac3efb",
106         "type": "Role"
107       }
108     ]
109   }
110 ],
111 "samlMetadataUrl": null,

```

**Note:**

- If your tenant is being created in **Azure Germany**, copy the entire content of [this file](#) and paste it into the section highlighted in the image above.
- If your tenant is being created in **Azure China**, copy the entire content of [this file](#) and paste it into the section highlighted in the image above.

22. Click **Save**.

23. Click **API permissions** from the left pane and click **Grant admin consent for <your\_company\_name>** option listed under *Grant consent* section. Grant the necessary permissions as required.

The API permission and its scope are available in [this table](#).

The screenshot shows the 'API permissions' page in the ManageEngine ADManager Plus interface. A confirmation dialog is displayed at the top, asking 'Grant admin consent confirmation. Do you want to grant consent for the requested permissions for all accounts in Zoho Corp? This will update any existing admin consent records this application already has to match what is listed below.' The 'Yes' button is highlighted. Below the dialog, a table lists the permissions granted for Zoho Corp.

API / Permissions name	Type	Description	Admin consent requ...	Status
<a href="#">Add a permission</a> <a href="#">Grant admin consent for Zoho Corp</a>				
<a href="#">Azure Active Directory Graph (2)</a>				
<a href="#">Microsoft Graph (11)</a>				
Application.ReadWrite.All	Application	Read and write all applications	Yes	Granted for Zoho Corp
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted for Zoho Corp
Calendars.Read	Application	Read calendars in all mailboxes	Yes	Granted for Zoho Corp
Directory.ReadWrite.All	Application	Read and write directory data	Yes	Granted for Zoho Corp
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for Zoho Corp
Policy.Read.All	Application	Read your organization's policies	Yes	Granted for Zoho Corp
Reports.Read.All	Application	Read all usage reports	Yes	Granted for Zoho Corp
RoleManagement.ReadWrite.Directory	Application	Read and write all directory RBAC settings	Yes	Granted for Zoho Corp
ServiceHealth.Read.All	Application	Read service health	Yes	Granted for Zoho Corp

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 ADManager 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. Go to **Certificates** and click **Upload certificate**. Upload your application certificate as a .cer file.

33. 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:** 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.

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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.

Upload certificate

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.

New client secret

Description	Expires	Value	ID
M365 Manager Plus	12/31/2299		198b5174-e56b-486a-8712-daae74bd838f

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

35. Copy the **Application (client) ID** and **Object ID** values and save them. You will need these values to configure your tenant in the ADManager Plus portal.

M365 Manager Plus

Search (Ctrl+/)

Delete

Endpoints

Preview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Essentials

Display name : M365 Manager Plus

Application (client) ID : 65a3f9cf-b034-42c1-ab72-edf5344b36dc

Directory (tenant) ID : 21b99734-6526-4f35-aa6b-5a76b085b4e3

Object ID : 21b99734-6526-4f35-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.

View API permissions

Documentation

Microsoft identity platform

Authentication scenarios

Authentication libraries

Code samples

Microsoft Graph

Glossary

Help and Support



## Steps to manually configure Microsoft 365 tenant in ADManager Plus

1. Open the ADManager Plus portal with the below 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 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.

2. Enter your **Tenant Name**. For example, test.onmicrosoft.com.
3. Paste the **Application (client) ID** and **Application Object ID** which were saved earlier in Step 35, in the respective fields.
4. Enter the **Application Secret Key** that was saved during Step 31.
5. Upload a .pfx file of the certificate that has been uploaded in the Azure portal. Refer to Step 33.
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**. The tenant will be added in ADManager Plus. If you wish to modify the details in it, click *Edit* Option once the configuration is listed and proceed to make the changes.
9. Click **Update** once the necessary modifications are done. The Rest API Access should now be *Enabled* for the configured account.

## Steps to update a service account in ADManager Plus

1. Now the service account must be configured. To do this, navigate to **Domain/Tenant Settings > Microsoft 365** and click the **edit** option under the *Actions* column.
2. Click the **edit** icon found near *Service Account Details*.

Service Account Details

Service account name

admpteam@zohoadapazure.onmicrosoft

Password

.....

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.

## Steps to create a self-signed certificate

1. Run the following command in PowerShell:  
**Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force -Scope process**
2. Now, run the *Create-selfsignedcertificate.ps1* script.
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 ADManager Plus, while the .cer file should be uploaded in the [Azure portal of your application](#).

## Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

### ManageEngine ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management.

For more information about ADManager Plus, visit [manageengine.com/products/ad-manager/](https://manageengine.com/products/ad-manager/).

\$ Get Quote

⬇ Download