ManageEngine M365 Manager Plus

# Microsoft 365 Tenant Configuration

www.microsoft365managerplus.com

## **Table of Contents**

Automatic Microsoft 365 tenant configuration	1
Steps to modify REST API permissions	3
Manual Microsoft 365 tenant configuration	5
Steps to create an Azure AD application	6
Steps to modify a Microsoft 365 tenant	10
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
How to configure an MFA-enabled service account	12
Steps to configure Trusted IPs	13
Steps to configure Conditional Access	13
Appendix	14
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.

Manager Plus Management & Reporting ~	License Jobs 🤽 TalkBack ? 😔 🛪
Dashboard Reports Management Automation Delegation Settings Support	O Tenant Settings
Configure I Authorize ManageEngine M365 and audit your Microsoft 36 Administrator to authorize. W Configure us	Microsoft 365 Tenant Manager Plus to manage, report, monitor, 5 environment. Please login as Global e do not store this credential. Learn more. Ing Microsoft 365 Login
<ul> <li><u>Click here</u> to configure tenant with an already</li> <li><u>Choose the appropriate Azure Environment</u> if y Government clouds.</li> </ul>	registered Ázure AD Application. bur tenant is created in Azure Germany,China or US

- 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.

Per	
	rmissions requested
Rev	view for your organization
territori Mil Harage Va	ManageEngine M365 Manager Plus
This your	application is not published by Microsoft or organization.
This	app would like to:
$\sim$	Access the directory as the signed-in user
Å	Allows the app to have the same access to information in the directory as the signed-in user.
1	This is a permission requested to access your data in
lf you all use review	accept, this app will get access to the specified resources for rs in your organization. No one else will be prompted to v these permissions.
Accep your c staten f <b>or yc</b> https:/	ting these permissions means that you allow this app to use lata as specified in their terms of service and privacy nent. The publisher has not provided links to their terms out to review. You can change these permissions at //myapps.microsoft.com. Show details
Does	this app look suspicious? Report it here

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.

Re	eview for your organization
Ma	nageEngine M365 Manager Plus1197161203 verified
Thi	s application is not published by Microsoft.
Thi	s app would like to:
$\sim$	Read and write domains
V	Read service health information for your organization
$\sim$	Read and write all applications
V	Read and write directory data
$\sim$	Read and write mail in all mailboxes
$\checkmark$	Read and write items in all site collections
V	Read all usage reports
V	Read all audit log data
V	Read and write all users' full profiles
$\sim$	Read and write all directory RBAC settings
V	Sign in and read user profile
lf yc all u revia	u accept, this app will get access to the specified resources for sers in your organization. No one else will be prompted to ew these permissions.
Acce you state for y http	spting these permissions means that you allow this app to use data as specified in their terms of service and privacy ement. The publisher has not provided links to their terms you to review. You can change these permissions at at 2/myapps microsoft.com. Show details
Doe	s 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.

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.

M365 N	Manager Pl	us) Managerr	nent & Reporting	Ŷ				License Jobs 🧍	🛡 TalkBack ? 🕴 🕶
Dashboard	Reports	Management	Automation	Delegation	Settings	Support			O Tenant Settings
Configured Mic	rosoft 365	Tenants 💿							
								+ Add New Tenant	Manage License
Actions	Tena	nt Name		Domains	REST API	Access	Service Account		Status
影らくに	<b>i</b>	onmicrosoft.com		8 Domains	Enabled				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 Azure AD admin center.
- 2. Click Azure Active Directory from the left pane.
- 3. Choose App registration under Manage.
- 4. Select All applications.

Home > .				
Azure Active Directory	App regis	trations 🖈 …		
<ul> <li>Overview</li> <li>Preview features</li> <li>Diagnose and solve problems</li> </ul>	<ul> <li>New registration   Endpoints   Troubleshooting   Refresh</li> <li>Starting June 30th, 2020 we will no longer add any new features to Azure will no longer provide feature updates. Applications will need to be upgravely a starting to the start of the</li></ul>	Lownload      Preview features      Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview features     Preview fe	e to provide technical support	and security updates but we
Manage Users Groups External Identities	All applications Owned applications Deleted applications	<sup>+</sup> ♥ Add filters		
Roles and administrators	17 applications found Display name ↑↓	Application (client) ID	Created on $~\uparrow\downarrow$	Certificates & secrets
Enterprise applications	534 54		27/05/2022	✓ Current
<ul> <li>Devices</li> <li>App registrations</li> </ul>	TE		19/06/2020	-
<ul> <li>Identity Governance</li> <li>Application proxy</li> </ul>	TE		20/05/2022	-
<ul> <li>Custom security attributes (Preview)</li> </ul>	TE I		31/05/2022	Current
Licenses			10/08/2021	Expired

- 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.

Home > App registrations >					
<del></del>		API permissions 🛷 …			×
Search (Ctrl+/)	🖔 Refresh 🕴 🖗 Got feedback?				
Overview	Grant admin consent confirm	mation.			
i Quickstart	Do you want to grant consent for the	e requested permissions for all accounts in		This will update any exist	ting admin consent records this application
🚀 Integration assistant	already has to match what is listed be	elow.			
Manage	Yes No				
Branding & properties	🕂 Add a permission 🗸 Grant adn	nin consent for			
Authentication	API / Permissions name T	ype Description	Admin consent requ	Status	
📍 Certificates & secrets	✓ Azure Active Directory Graph (1)				
Token configuration	Domain.ReadWrite.All A	Application Read and write domains	Yes	Granted for	
<ul> <li>API permissions</li> </ul>	Microsoft Graph (10)				
Expose an API	AccessReview.Read.All A	Application Read all access reviews	Yes	A Not granted	
App roles	Application.ReadWrite.All A	Application Read and write all applications	Yes	Granted for	•••
A Owners	AuditLog.Read.All	Application Read all audit log data	Yes	<ul> <li>Granted for</li> </ul>	•••
& Roles and administrators	Directory.ReadWrite.All A	Application Read and write directory data	Yes	Granted for	
🔟 Manifest	Mail.ReadWrite A	Application Read and write mail in all mailboxes	Yes	<ul> <li>Granted for</li> </ul>	•••
Support + Troubleshooting	Reports.Read.All A	Application Read all usage reports	Yes	<ul> <li>Granted for</li> </ul>	•••
Troubleshooting	RoleManagement.ReadWrite.Dir	Application Read and write all directory RBAC settings	Yes	Granted for	
	Condeal Isalth Dood All		W= -	A Granted for	···· v

- 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.

	Microsoft Graph https://graph.microsoft.com/ Docs 🗗	
Vhat t	ype of permissions does your application require?	
Deleg Your	gated permissions 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.
e <mark>lec</mark> t	permissions	expand all
🔎 Sta	rt typing a permission to filter these results	
Pe	ermission	Admin consent required
	ccessReview (1)	
	AccessReview.Read.All ① Read all access reviews	Yes
	AccessReview.ReadWrite.All ① Manage all access reviews	Yes
	AccessReview.ReadWrite.Membership ① Manage access reviews for group and app memberships	Ves

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.** 

ManageEngine Moos	manag			Other permissions have been granted
⊘ Refresh				this tenant that are not configured. Learn m
A You are editing permission(s) to your	application, us	ers will have to consent even if they've already done so	previously.	Do you want to keep these other granted permissions?
Configured permissions				• Yes, add other granted permissions to
Applications are authorized to call APIs will all the permissions the application needs.	hen they are o Learn more a	granted permissions by users/admins as part of the bout permissions and consent	consent process. The list of c	No, remove other granted permissions
+ Add a permission 🗸 Grant admir	n consent for			
API / Permissions name	Туре	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	
		Read and write mail in all mailboxes	Yes	
Mail.ReadWrite	Application			
Mail.ReadWrite Reports.Read.All	Application Application	Read all usage reports	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

Azure AD Application will be	e used to collect data via Microsoft Gra	ph API. Please provide the
details	of an application with sufficient permis	sions.
Application Details		How to Configure?
* Tenant Name		
* Application ID		
* Application Object ID		
Application Secret & Certifi	cate ⑦	
* Application Secret Key		
* Application Certificate	No file selected B	rowse 🕐
		(?)
	Upload PFX certificate(.pfx) file	
	Add Tenant Cancel	
chere to configure tenant usi	ing Microsoft 365 Login	

## 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 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 and 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

→ M365 Manager Plus	s   Authentication 🛷	
	🔚 Save 🗙 Discard 🛛 🛇 Got feedback?	
Overview	Platform configurations	
🍊 Quickstart	Plation conligurations	
🚀 Integration assistant	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.	
Manage	+ Add a platform	
🔤 Branding		
Authentication	∧ Web Quickstart Docs c⅔	Ŵ
📍 Certificates & secrets	Redirect URIs	
Token configuration	The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as	
<ul> <li>API permissions</li> </ul>	reply URLs. Learn more about Redirect URIs and their restrictions <sup>2</sup>	
<ul> <li>Expose an API</li> </ul>	https://manageengine.com/office365-management-reporting/redirect.html	Ŵ
App roles   Preview	https://demo.o365managerplus.com/oauth/redirect	Ŵ
Owners	http://localhost.8365/webclient/GrantAccess	Ŵ
Roles and administrators   Preview	http://localhost8365/webclient/VerifyUser	Ŵ
III Manifest	https://identitymanager.manageengine.com/api/public/v1/oauth/redirect	Û
Support + Troubleshooting	Add URI	

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.



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.



- 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.

Manage						
Branding	Certificates					
Authentication     ■	Certificates can be used as secrets to prove the	application's identity	when requesting a toke	n. Also can be referred to	as public keys.	
📍 Certificates & secrets	↓ Upload certificate					
Token configuration	Thumborint		Start date	Evnires	חו	
API permissions	manopina		Start date	Lypnes		
🙆 Expose an API	No certificates have been added for this application	ation.				
App roles   Preview						
Owners	Client cocrete					
Roles and administrators   Preview	Clefit secrets					
0 Manifest	A secret string that the application uses to prov	e its identity when re	questing a token. Also c	an be referred to as appli	cation password.	
Support + Troubleshooting	+ New client secret					
<i>Troubleshooting</i>	Description	Expires	Value		ID	
New support request	M365 Manager Plus	12/31/2299			198b5174-e56b-486a-87	712-daee74bd838f 🗈 📋

- 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.

🔣 M365 Manager Plus	#		
Search (Ctrl+/) «	💼 Delete 🔀 Endpoints 🖼 Preview features		
Overview	▲ Essentials		
😃 Quickstart	Display name : M365 Manager Plus	Supported account types	: My organization only
💉 Integration assistant	Application (client) ID : 85e3f9cf-b034-42c1-ab72-edf5344b36dc	Redirect URIs	: 4 web, 0 spa, 0 public client
	Directory (tenant) ID :	Application ID URI	: Add an Application ID URI
Manage	Object ID : d1b99734-6526-4735-aa6b-5a76b085b4e3	Managed application in I	: M365 Manager Plus
Branding	A Station lune 37th - 1370 un will do loader and an usual features to Anno Athen Directory Authoritical Berny (ADAI) and Anno AD Grade Mile will evolute to envide to behavior to envide technical curves of security under	s but we will be lenges provide	fosturo undator. Applications will
Authentication	Starting June Sont, 2020 we will no longer aud any new reactives to Azure Active Directory Autoentication Library (ADAC) and Azure AD Graphi, we will continue to provide recrimical support and security update	s but we will no longer provide	reature updates. Applications will
📍 Certificates & secrets			
Token configuration	Call APIs	Documentation	
API permissions		Microsoft identity platform	
🙆 Expose an API		Authentication scenarios Authentication libraries	
App roles   Preview		Code samples Microsoft Graph	
Owners		Glossary Help and Support	
Roles and administrators   Preview	Build more powerful apps with rich user and business data	Thep and Support	
10 Manifest	from Microsoft services and your own company's data sources.		
Support + Troubleshooting	View API permissions		

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.

M365 Manager Plus								License Jobs 单	TalkBack ? 😌
	Reports	Management		Delegation	Settings	Support			O Tenant Setting
Configured Mice	Configured Microsoft 365 Tenants 💿								
								+ Add New Tenant	Manage License
Actions	Ter	nant Name		Domains		REST API Access	Service Account		Status
₩ Ə 🖊 i	ê & <b>E</b>	.onmicrosoft.con	n	48 Domain	15	Enabled	onmicrose	oft.com	Success

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

nouny Application Details		- DBCK
Application Details		How to Configure
* Application (Client) ID		
* Application Object ID		
Application Secret & Certificate ③		
* Application Secret Value		
* Application Certificate	No file selected Bro	wwse 🕐
		0

- 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.

details o	of an application with sufficient permissions.
Application Details	How to Config
* Tenant Name	
* Application ID	
* Application Object ID	
Application Secret & Certific	cate 🕐
* Application Secret Key	
* Application Certificate	No file selected Browse ⑦
	3
	Upload PFX certificate(.pfx) file
	Add Tenant Cancel

- 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 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 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
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.
- 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.
		AdminsitrativeUnit. 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.

Auditing and Alerting	Office 365 Management	ActivityFeed.Read	Get audit reports and alerts.
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.

#### **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/.

\$ Get Quote

**±** Download