

ManageEngine
ADAudit Plus

Azure AD configuration guide

www.adauditplus.com

Table of contents

1. Overview	1
2. Comparing the methods for configuring Azure AD	2
3. Configuring Azure AD in ADAudit Plus	3
3.1 Configuring using Azure AD premium license	3
3.2 Configuring using a Microsoft 365 license	13
4. Reporting capabilities of ADAudit Plus	27
4.1 ADAudit Plus vs. Azure portal	27
4.2 ADAudit Plus vs. PowerShell cmdlets	28
5. Event categories tracked by ADAudit Plus	28
5.1 Event details	28
6. Log retention settings in Azure AD	29
7. Troubleshooting	29

1. Introduction

Enforce accountability and enhance security across your Microsoft Azure Active Directory (AD) environment using ManageEngine's UBA-driven change auditing solution, ADAudit Plus. It helps keep track of the changes made to various AD objects, as well as authentication attempts, to ensure compliance with regulatory mandates such as PCI DSS, HIPAA, and the GDPR.

Highlights of auditing Azure AD using ADAudit Plus

- Gain complete visibility into your on-premises, cloud, or hybrid AD environment from a single console.
- Audit and record both failed and successful authentication attempts and analyze authentication patterns across both on-premises and cloud AD environments.
- Protect your organization from various IT security threats by analyzing high-risk activities, such as when a user logs in to a disabled application or tries to sign in using a disabled account.
- Track and report on all changes in a user account's life cycle, including creation, deletion, enabling, disabling, and restoration.
- Audit and alert on every time a user is added or removed from a device.
- Locate and analyze members who are added or removed from AD groups and prevent privilege misuse.
- Meet the required security standards across Azure tenants by keeping a close eye on recently added or removed OneAuth permissions.
- Track and analyze the usage of Azure applications and the failed requests.
- Trigger instant email or SMS notifications every time Azure AD multi-factor authentication (MFA) fails.

This guide takes you through the process of setting up ADAudit Plus to audit an Azure AD environment.

2. Comparing the methods for configuring Azure AD

ADAudit Plus offers two methods to audit your Azure environment. They are:

- Using an Azure AD Premium license.
- Using a Microsoft 365 license.

Category	Azure	Microsoft 365
Geolocation	Possible	Not possible
MFA details	Possible	Not possible
Group-based license change	Possible	Not possible
Application display name	Possible	Possible by using the Azure AD module
Modified properties, along with their new and old values	Possible	Not possible with basic edition of Microsoft 365 E1 licensing
Sign-in risk detection and reporting	Possible	Not possible

Table 1: A detailed comparison of how auditing Azure varies depending on whether you use a Microsoft 365 license or an Azure AD Premium license.

Note: ADAudit Plus strongly recommends the use of an Azure AD Premium license over a Microsoft 365 license to get more features.

3. Configuring Azure AD in ADAudit Plus

3.1. Configuring using Azure AD premium license

To audit your Azure AD environment using an Azure AD Premium license, ADAudit Plus uses the Microsoft Graph API to obtain events from Azure AD.

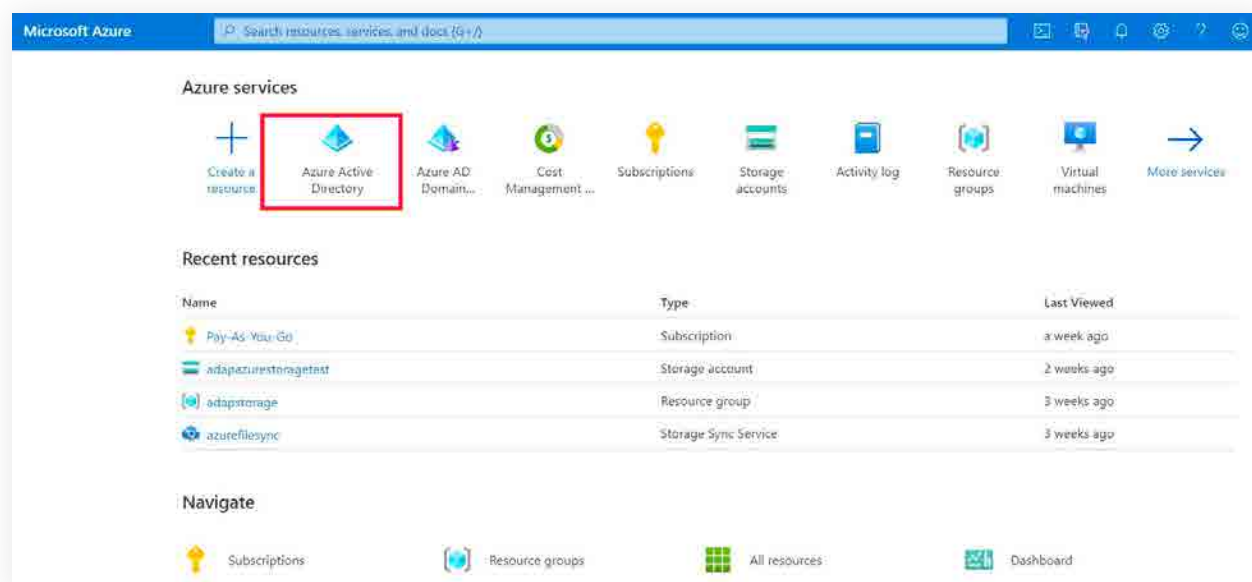
Privileges required while using Microsoft Graph API

- Application.Read.All
- AuditLog.Read.All
- Directory.Read.All
- IdentityRiskEvent.Read.All
- Group.Read.All
- User.Read.All

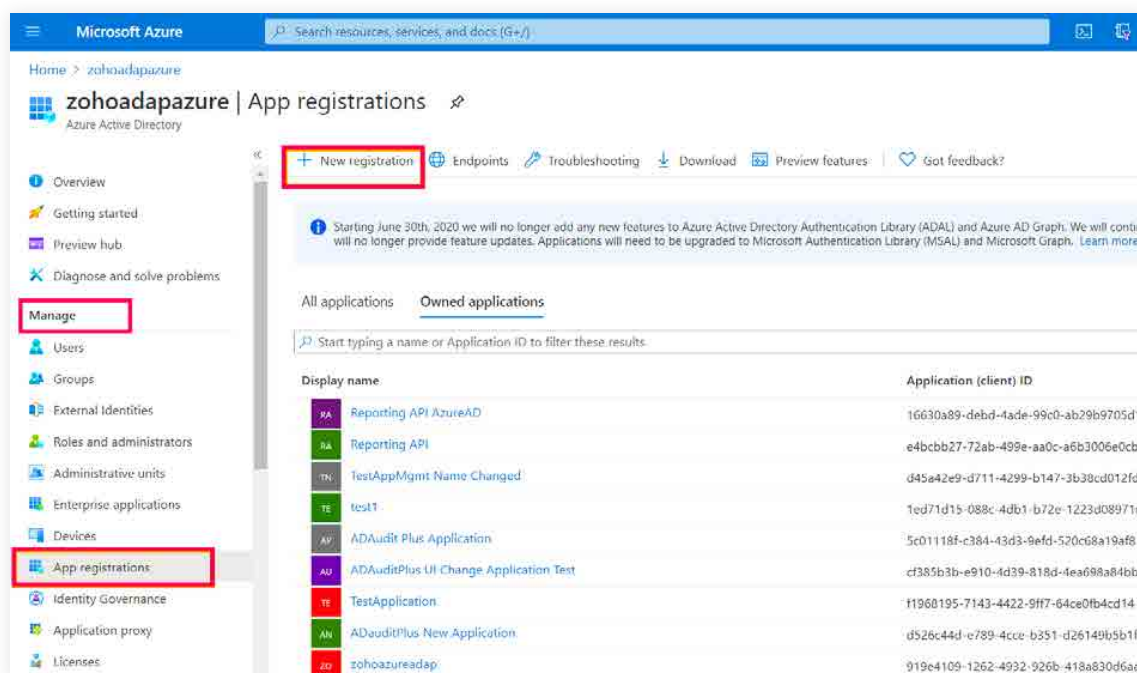
Register an application

Register an application in the Azure portal, using these steps:

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select **Azure Active Directory** from the Azure services section.



3. Go to **Manage > App registrations > New registrations** to open the Register an application window.



4. Enter the **application name**, for example, **AD Audit Plus Application**.
5. Ensure that **Accounts in this organizational directory only (zohoadapazure only - Single tenant)** is selected under **Supported account types**.

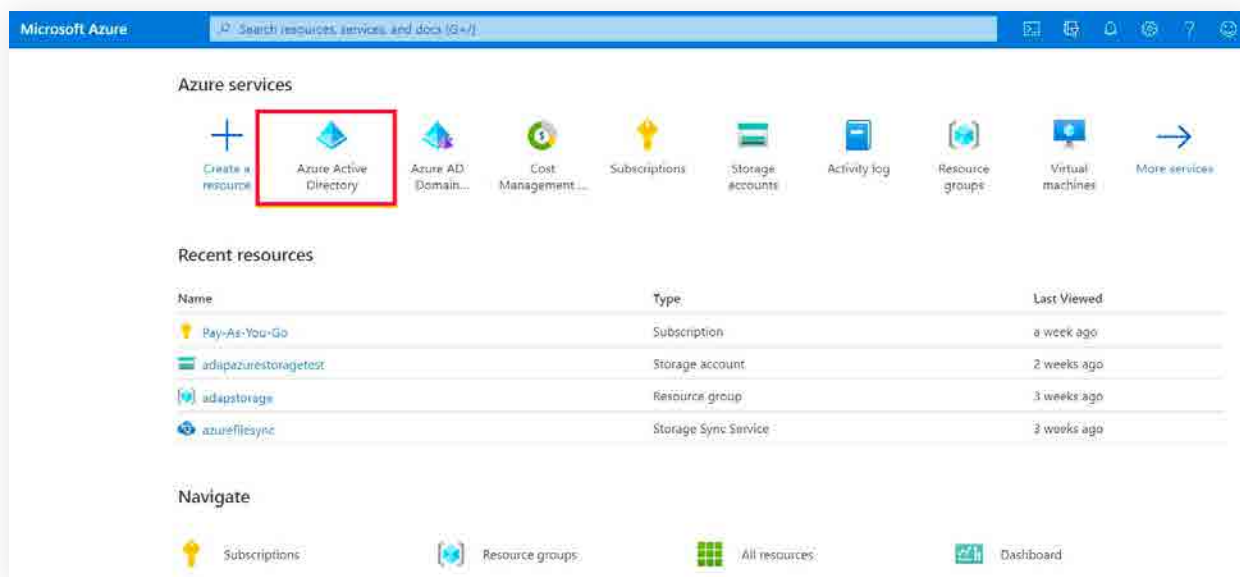
The screenshot shows the 'Register an application' form in the Microsoft Azure portal. The 'Name' field is filled with 'AD Audit Plus application'. Under the 'Supported account types' section, the option 'Accounts in this organizational directory only (zohoadapazure only - Single tenant)' is selected and highlighted with a red box. The 'Register' button at the bottom is also highlighted with a red box. The form includes a 'Redirect URI (optional)' field with a dropdown menu set to 'Web' and a text input field containing 'e.g. https://myapp.com/auth'. A checkbox at the bottom indicates agreement to the Microsoft Platform Policies.

6. Click **Register**.

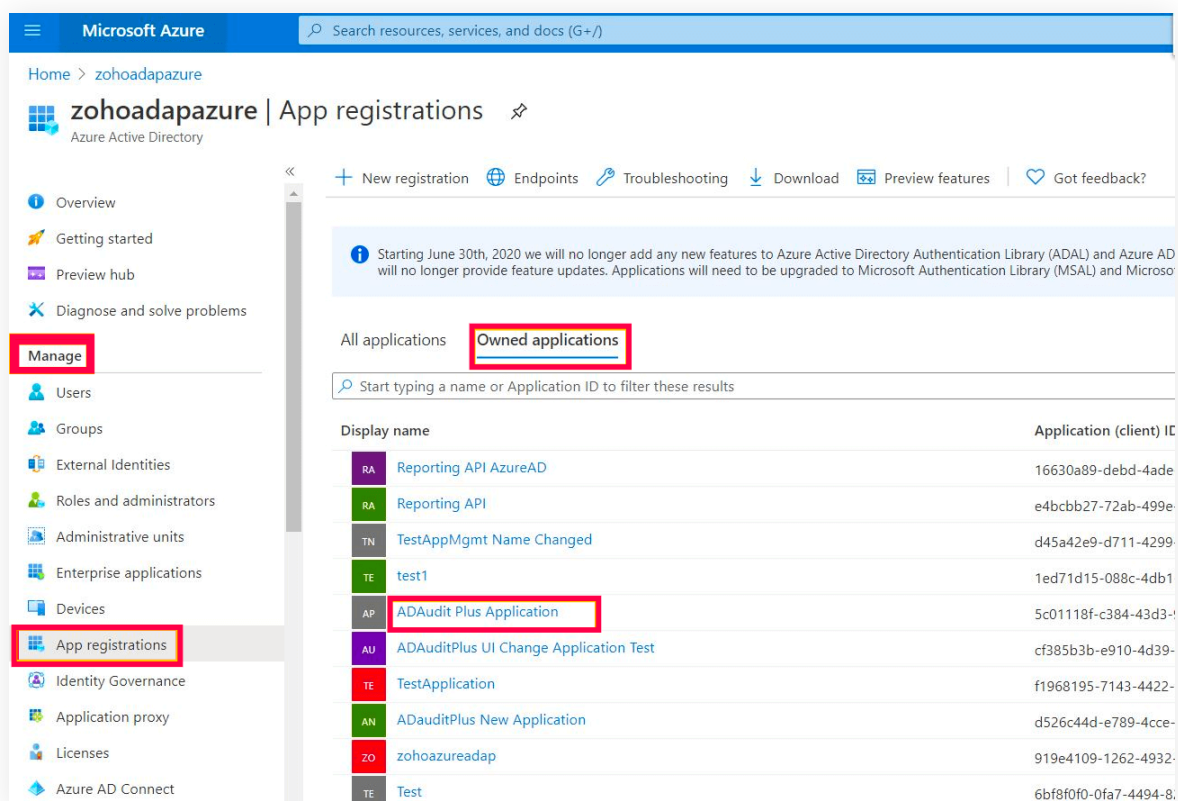
Grant minimum privileges required for Microsoft Graph API

To grant the necessary privileges using Microsoft Graph API:

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select **Azure Active Directory** from the Azure services section.



3. Go to **Manage > App registrations**. Select your application under Owned applications.



4. Go to **Manage > API permissions** and select **+ Add a permission**.

Microsoft Azure

Home > zohoadapazure > ADAudit Plus Application

ADAudit Plus Application | API permissions

Search (Ctrl+/) « Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview
Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview
Manifest

This application is using Azure AD Graph API, which is on a deprecation path. Starting June 30th, 2020 we will no longer add any new application to use Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The application needs all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for zohoadapazure

API / Permissions name	Type	Description	Admin consent
▼ Azure Active Directory Graph (1)			
Directory.Read.All	Application	Read directory data	Yes
▼ Microsoft Graph (3)			
AuditLog.Read.All	Application	Read all audit log data	Yes
Directory.Read.All	Application	Read directory data	Yes
User.Read	Delegated	Sign in and read user profile	-

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

5. Select **Microsoft Graph**. Click **Application permissions** as the type of permission required.

6. From the listing, select the following:

- Application.Read.All
- AuditLog.Read.All
- Directory.Read.All
- IdentityRiskEvent.Read.All
- Group.Read.All
- User.Read.All

Request API permissions

< All APIs

> APIConnectors

Application (1)

<input checked="" type="checkbox"/>	Application.Read.All ⓘ Read all applications	Yes
<input type="checkbox"/>	Application.ReadWrite.All ⓘ Read and write all applications	Yes
<input type="checkbox"/>	Application.ReadWrite.OwnedBy ⓘ Manage apps that this app creates or owns	Yes

> AppRoleAssignment

> ApprovalRequest

AuditLog (1)

<input checked="" type="checkbox"/>	AuditLog.Read.All ⓘ Read all audit log data	Yes
-------------------------------------	--	-----

> BitlockerKey

Add permissions Discard

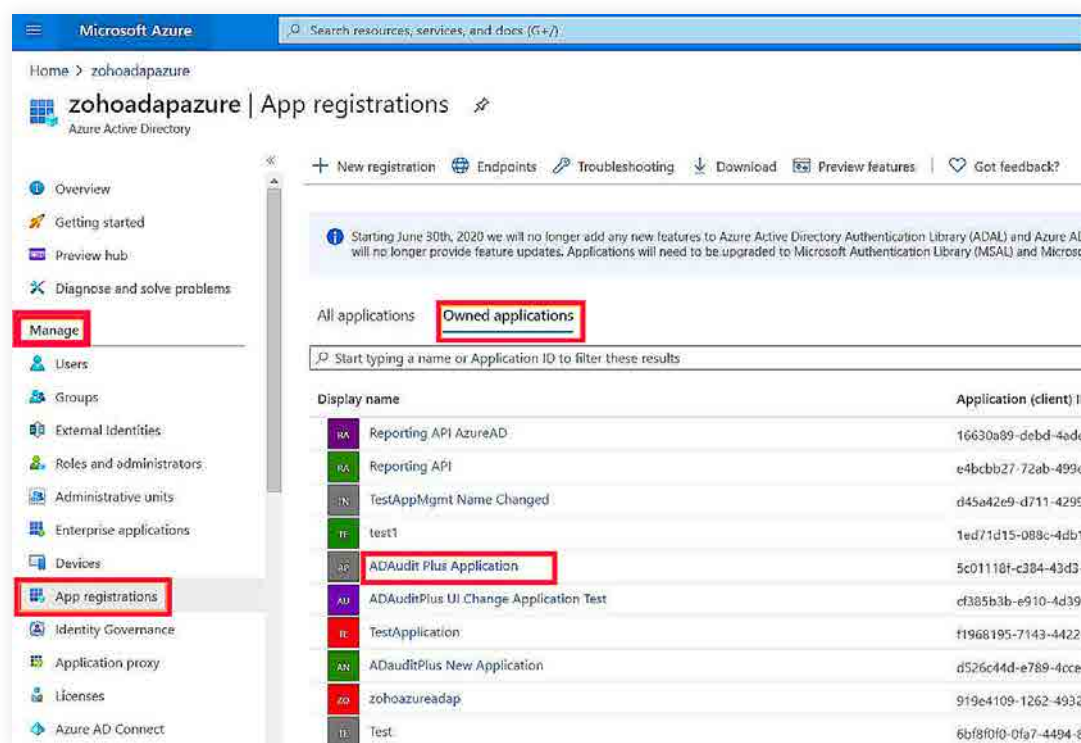
7. Click **Add permissions**.

8. Select **Grant admin consent for <tenantname>**

9. Click **Yes**.

Obtain client ID and client secret

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select **Azure Active Directory** service from the Azure services section.
3. Go to **Manage > App registrations**. Select your **application** under Owned applications.



4. Go to **Manage > Certificates & secrets**.
 - Click **+ New client secret**.
 - Enter the **description**.
 - Choose **24 Months** as the expiration date; this is the maximum value that can be used.
 - Click **Add**.
 - Copy the client secret value (e.g., "14uCILxkHtIVGR3wkCq12341Nd5VtestkkWTyIPrrE=")

Microsoft Azure

Search resources, services, and docs (G+/)

Home > zohoadapazure > ADAudit Plus applicaiton

ADAudit Plus application | Certificates & secrets

Search (Ctrl+/)

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens (instead of a client secret). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

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

Upload certificate

Thumbprint	Start date	Expires
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 a credential.

New client secret

Description	Expires	Value
No client secrets have been created for this application.		

Microsoft Azure

Search resources, services, and docs (G+/)

Home > zohoadapazure > ADAudit Plus applicaiton

ADAudit Plus application | Certificates & secrets

Search (Ctrl+/)

Got feedback?

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

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

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

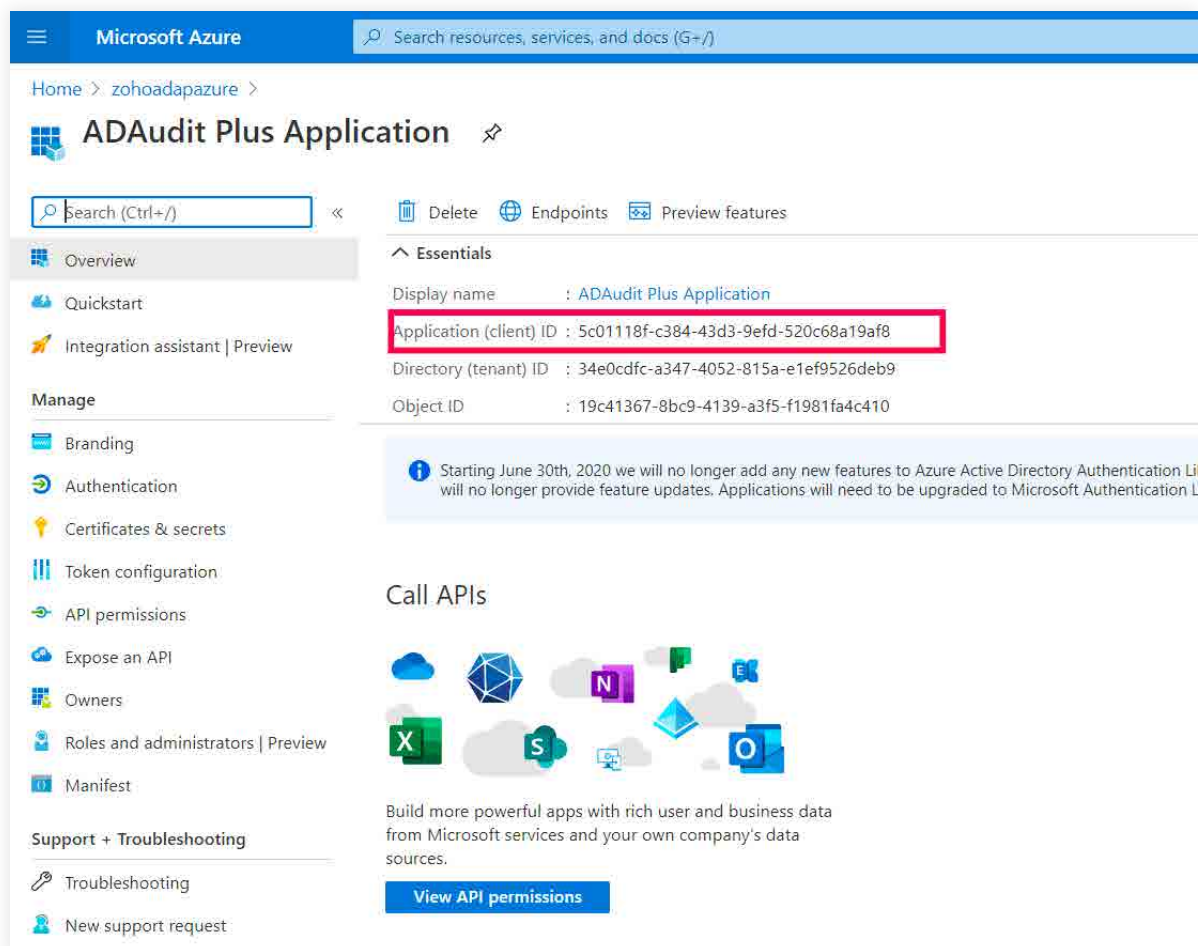
Client secrets

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

New client secret

Description	Expires	Value
ADAudit Plus application description	11/16/2021	opGY.mZrq_9kpXvh9aLLn~21tdH0~h1JG_

5. Go to **Manage > App registrations**. Select your application under *Owned Applications*.
6. Navigate to *Application (Client ID)* and click **Copy to clipboard**.



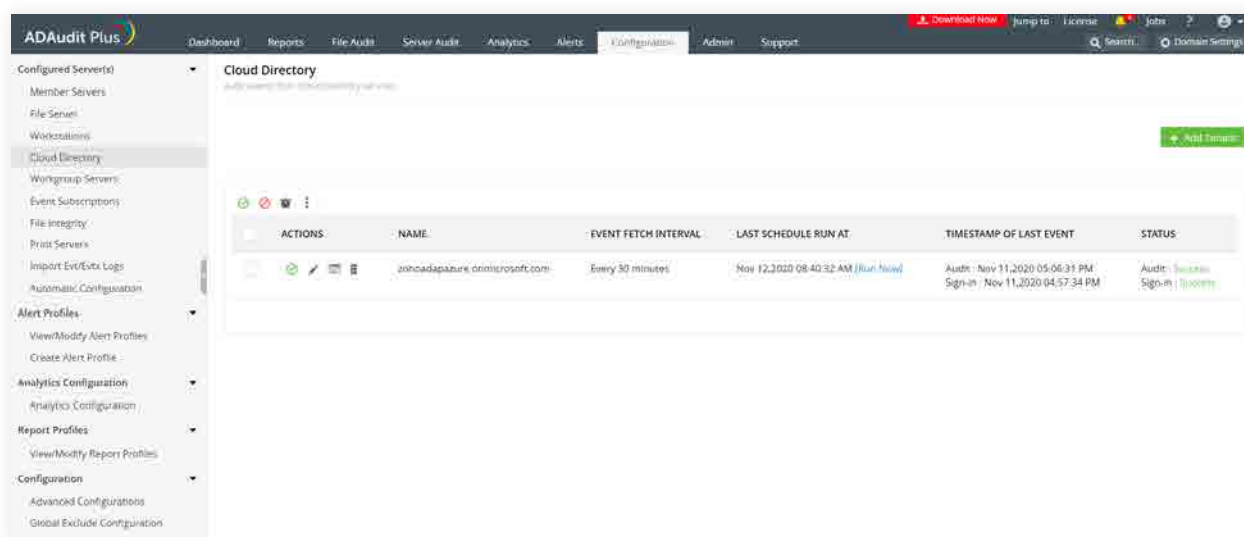
The screenshot shows the Microsoft Azure portal interface for an application named 'ADAudit Plus Application'. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant | Preview, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'ADAudit Plus Application' and includes a search bar and action buttons (Delete, Endpoints, Preview features). Under the 'Essentials' section, the following details are listed:

- Display name : ADAudit Plus Application
- Application (client) ID : 5c01118f-c384-43d3-9efd-520c68a19af8 (highlighted with a red box)
- Directory (tenant) ID : 34e0cdfc-a347-4052-815a-e1ef9526deb9
- Object ID : 19c41367-8bc9-4139-a3f5-f1981fa4c410

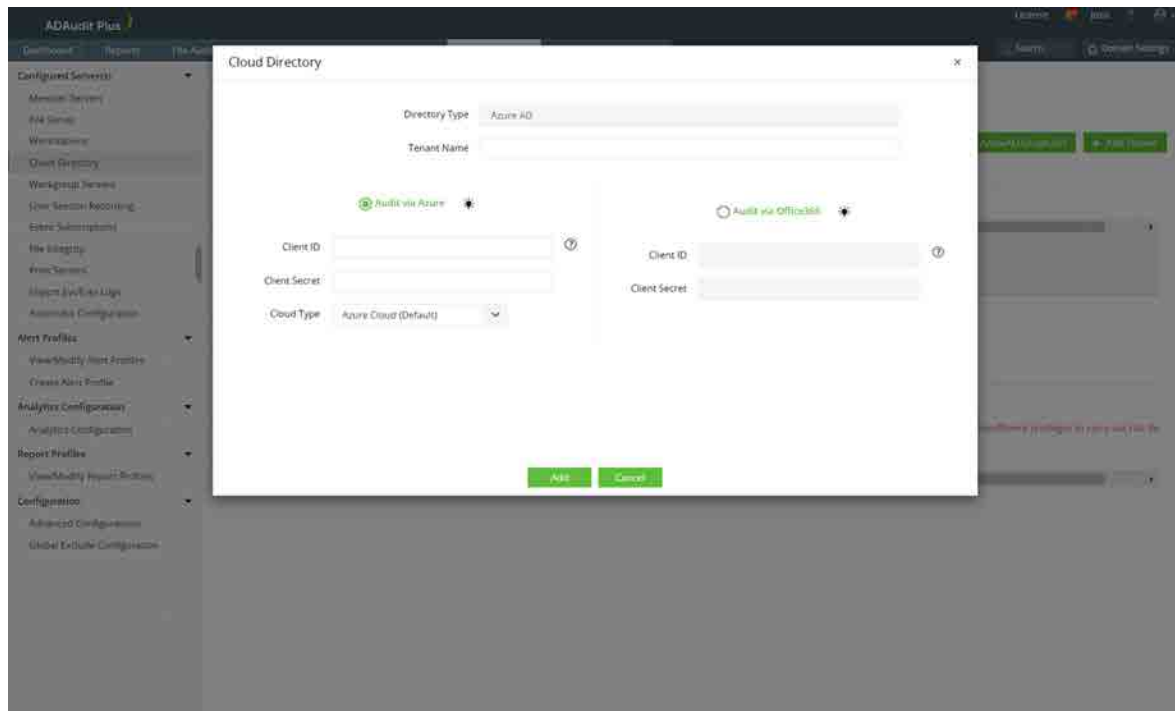
A blue information banner states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL). We will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL).' Below this, the 'Call APIs' section features icons for various Microsoft services (OneDrive, SharePoint, Teams, Outlook, etc.) and a button labeled 'View API permissions'.

Setting up Azure AD in ADAudit Plus

1. Open the **ADAudit Plus** web console.
2. Go to **Configuration > Configured Server(s) > Cloud Directory**.
3. Select **+Add Tenant** in the top-right corner.



4. Select **Audit via Azure**.
5. In the *Cloud Directory* window, choose the **Cloud Type** based on the national cloud points from the list below:
 - Azure AD global service (Azure Cloud - Default)
 - Azure AD for US Government L4 (Azure GCC High Cloud)
 - Azure AD for US Government L5 (Azure DOD Cloud)
 - Azure AD China operated by 21Vianet (Azure China Cloud)
 - Azure AD for Germany (Azure Germany Cloud)
6. Enter the **Tenant Name**, **Client ID**, and **Client Secret**.



7. Click **Add**.

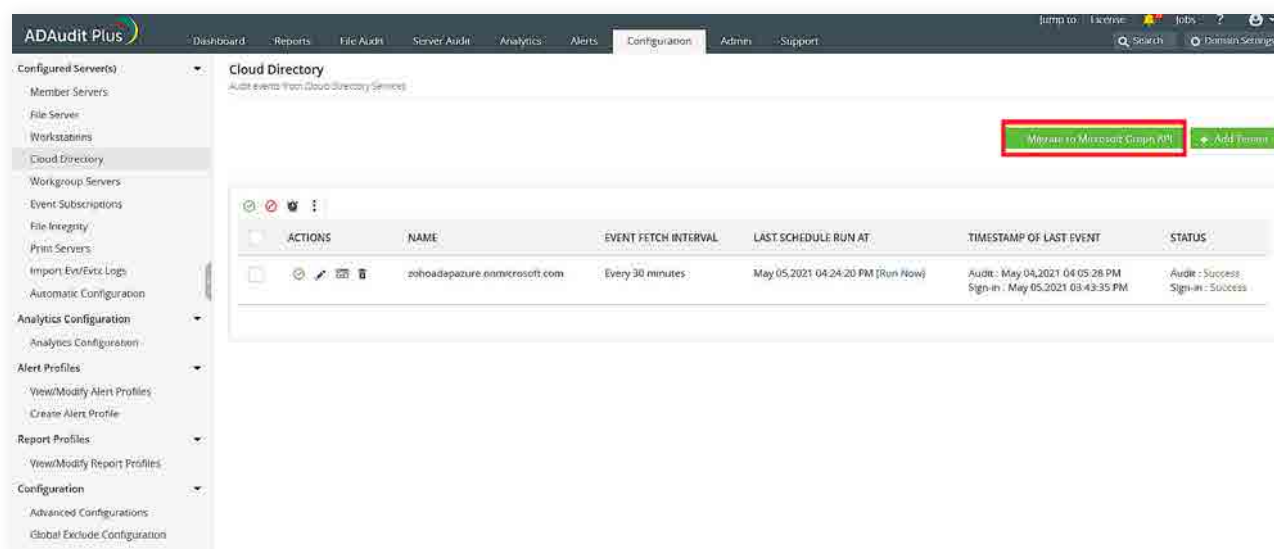
Privileges required while using Azure AD Graph API

The use of Azure AD Graph API is deprecated. Instead, it's strongly recommended you use the Microsoft Graph API to audit your Azure AD.

For more details on why Azure AD graph API was deprecated, check the [FAQ](#).

Check if you are using Azure AD Graph API and, if so, migrate using these steps:

1. Open the **ADAudit Plus web console**.
2. Go to **Configuration > Configured Server(s) > Cloud Directory**.
 - In the top-right corner, if the **Migrate to Microsoft Graph API** button is available, then Azure Active Directory Graph API is in use.
 - If the **Back to Azure AD Graph API** button is available, then Microsoft Graph API is in use.
3. Migrate to Microsoft Graph API from Azure AD Graph API by clicking **Migrate to Microsoft Graph API** at the top-right corner.
4. Click **Yes** in the confirmation prompt.



Note: Once you have migrated to Microsoft Graph API, add the necessary minimum privileges using the steps listed [here](#).

If you still want to use Azure AD Graph API, you can find the privileges required below:

- Directory.Read.All

3.2. Configuring using a Microsoft 365 license

To audit your Azure AD environment using a Microsoft 365 license, ADAudit Plus uses the Microsoft 365 Management API for all installations after ADAudit Plus build 7050.

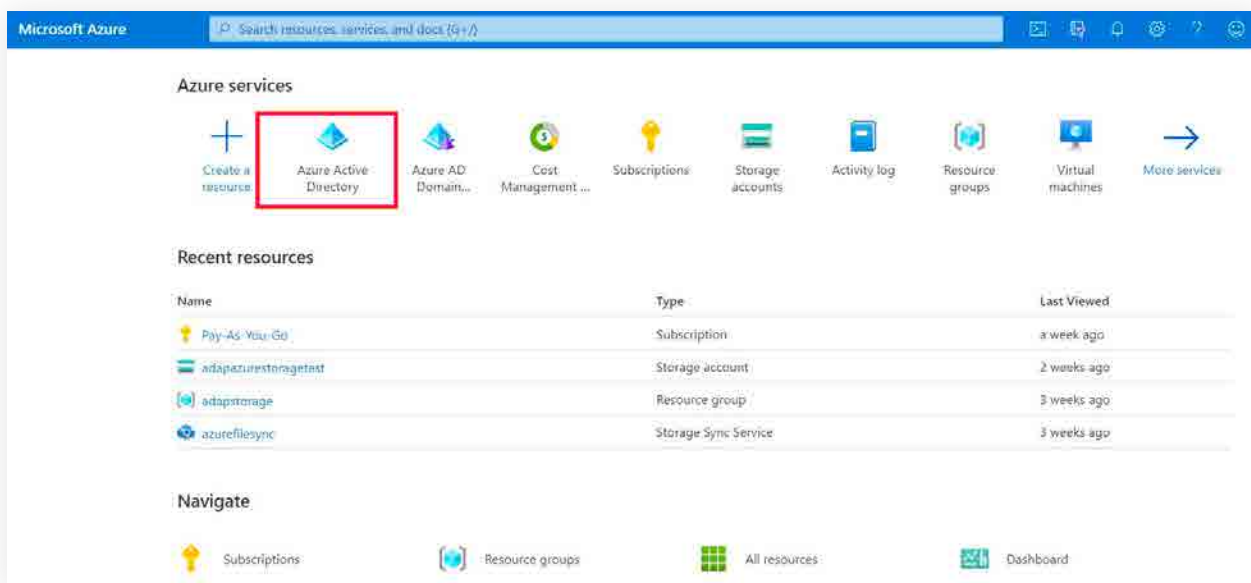
Privileges required while using Microsoft 365 Management API

- Microsoft Graph API > Directory.Read.All
- Office 365 Management API > ActivityFeed.Read

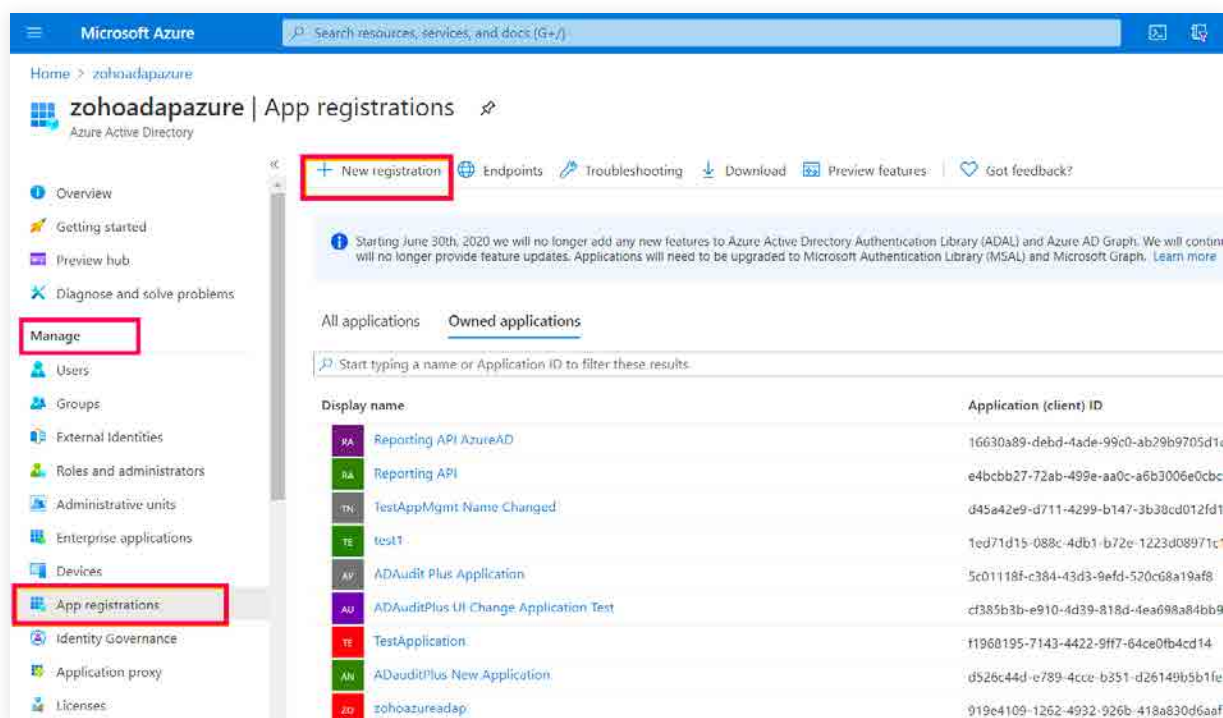
Register an application

Register an application in the Azure portal, using these steps:

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select the **Azure Active Directory** service from the Azure services top pane.



- Go to **Manage > App registrations > New registrations** to open the Register an application window.



- Enter the **application name**, for example, **AD Audit Plus Application**.
- Ensure that **Accounts in this organizational directory only (zohoadapazure only - Single tenant)** is selected under **Supported account types**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > zohoadapazure >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

ADAudit Plus application ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (zohoadapazure only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

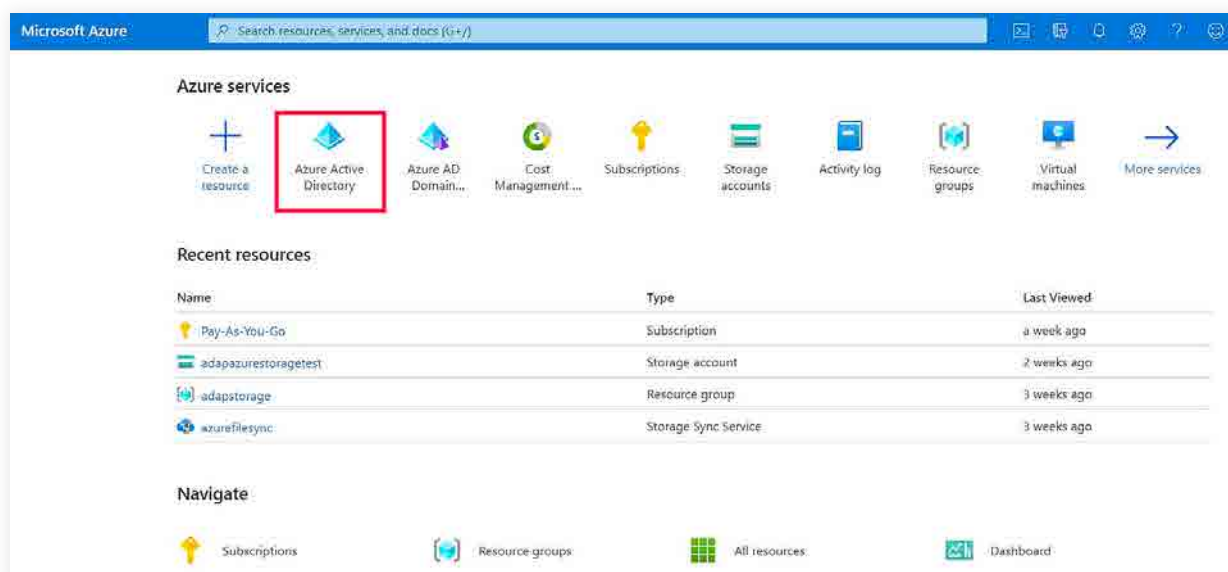
Register

6. Click **Register**.

Grant minimum privileges required for Microsoft 365 Management API

Grant the necessary privileges using Microsoft 365 Management API, using these steps:

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select **Azure Active Directory** service from the Azure services section.



- Go to **Manage > App registrations**. Select **your application** under Owned applications.

Microsoft Azure

Home > zohoadapazure

zohoadapazure | App registrations

Overview
Getting started
Preview hub
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect

+ New registration | Endpoints | Troubleshooting | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microso

All applications | **Owned applications**

Start typing a name or Application ID to filter these results

Display name	Application (client) ID
RA Reporting API AzureAD	16630a89-debd-4ade
RA Reporting API	e4bcbb27-72ab-499e
TN TestAppMgmt Name Changed	d45a42e9-d711-4299
TE test1	1ed71d15-088c-4db1
AP ADAudit Plus Application	5c01118f-c384-43d3-
AU ADAuditPlus UI Change Application Test	cf385b3b-e910-4d39-
IE TestApplication	f1968195-7143-4422-
AN ADAuditPlus New Application	d526c44d-e789-4cce-
ZO zohoadapazure	919e4109-1262-4932-
TE Test	6bf8f0f0-0fa7-4494-8-

- Go to **Manage > API permissions** and select **+ Add a permission** to open the Request API permissions window.

Microsoft Azure

Home > zohoadapazure > ADAudit Plus Application

ADAudit Plus Application | API permissions

Search (Ctrl+/) | Refresh | Got feedback?

Overview
Quickstart
Integration assistant | Preview
Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview
Manifest

This application is using Azure AD Graph API, which is on a deprecation path. Starting June 30th, 2020 we will no longer add any n application to use Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. [Learn more](#)

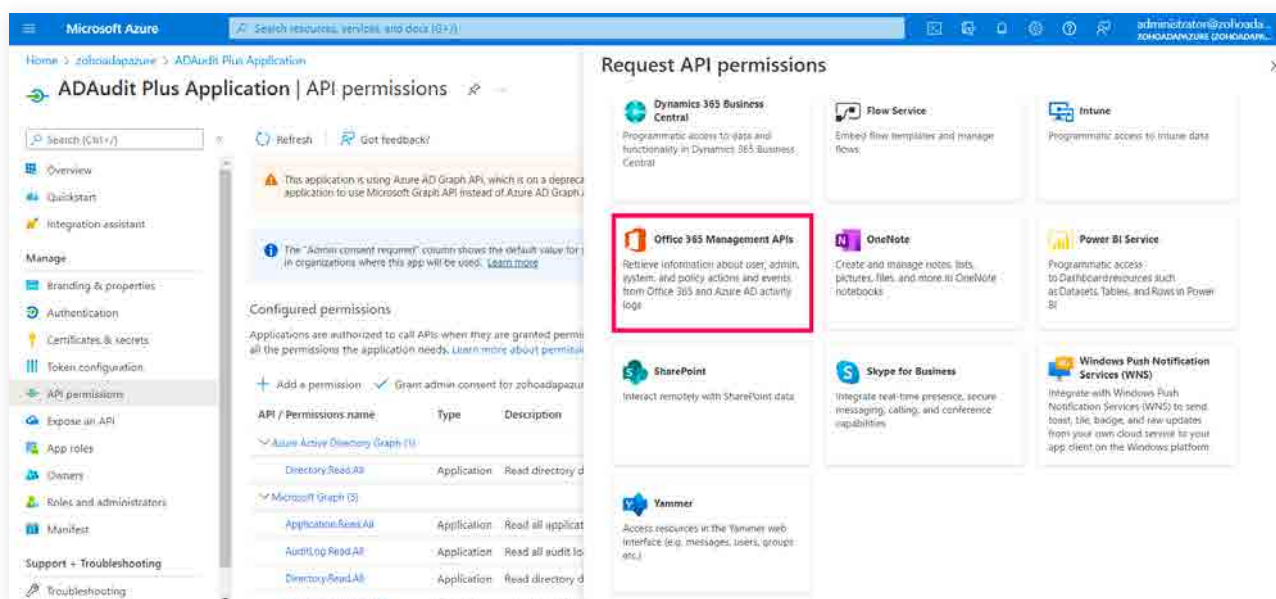
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The all the permissions the application needs. [Learn more about permissions and consent](#)

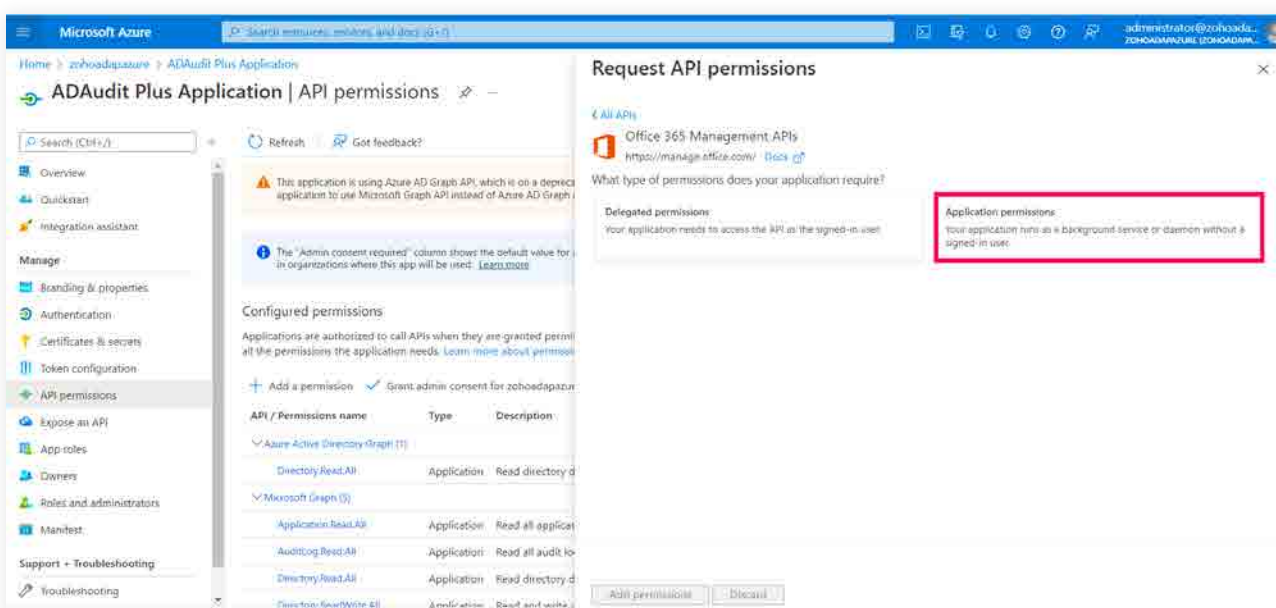
+ Add a permission | Grant admin consent for zohoadapazure

API / Permissions name	Type	Description	Admin cons
Azure Active Directory Graph (1)			
Directory.Read.All	Application	Read directory data	Yes
Microsoft Graph (3)			
AuditLog.Read.All	Application	Read all audit log data	Yes
Directory.Read.All	Application	Read directory data	Yes
User.Read	Delegated	Sign in and read user profile	-

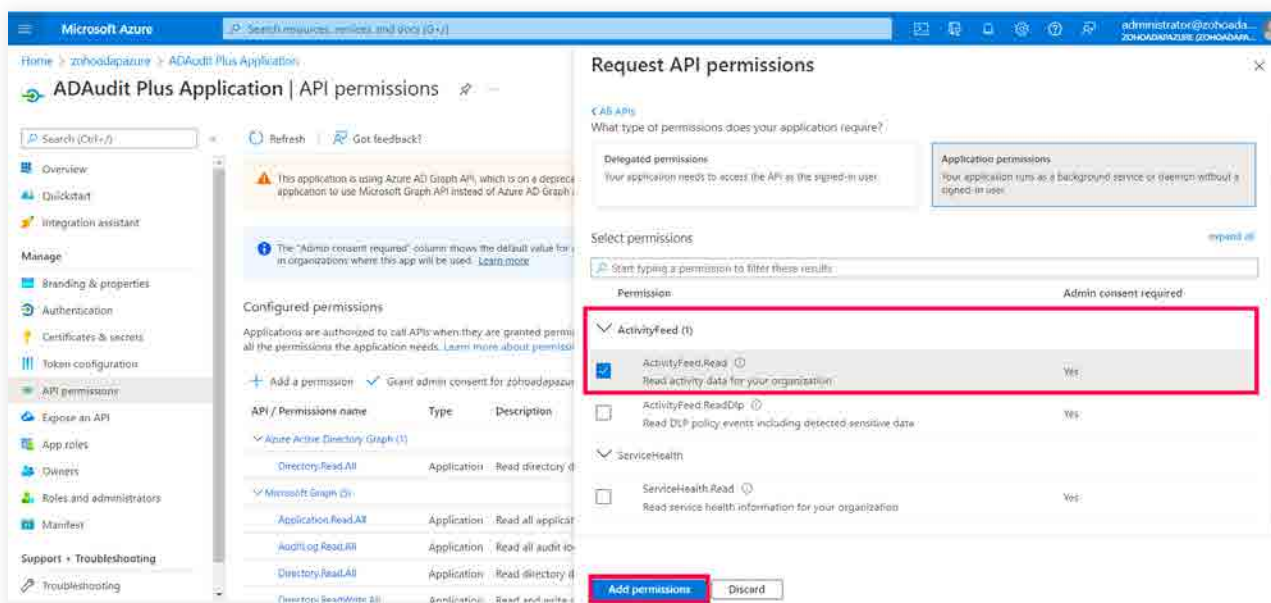
5. Select Office 365 Management APIs.



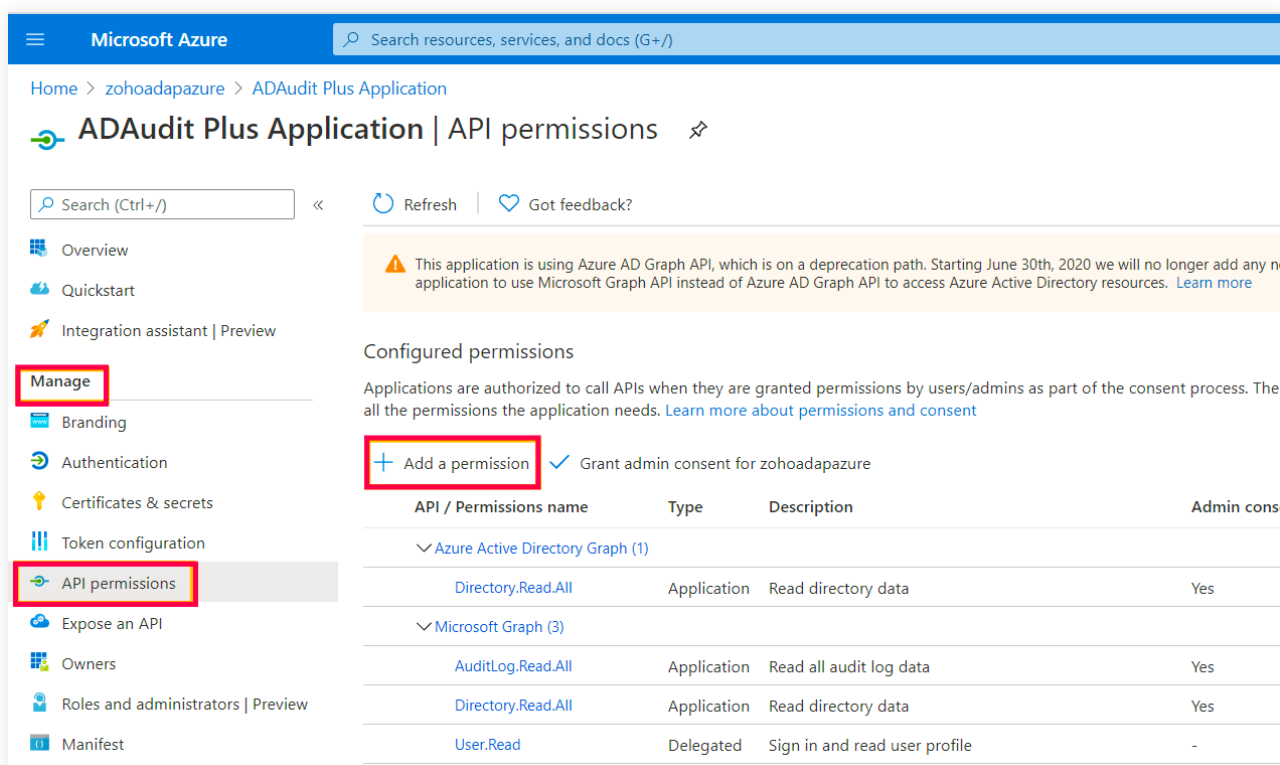
6. Choose Application permissions.



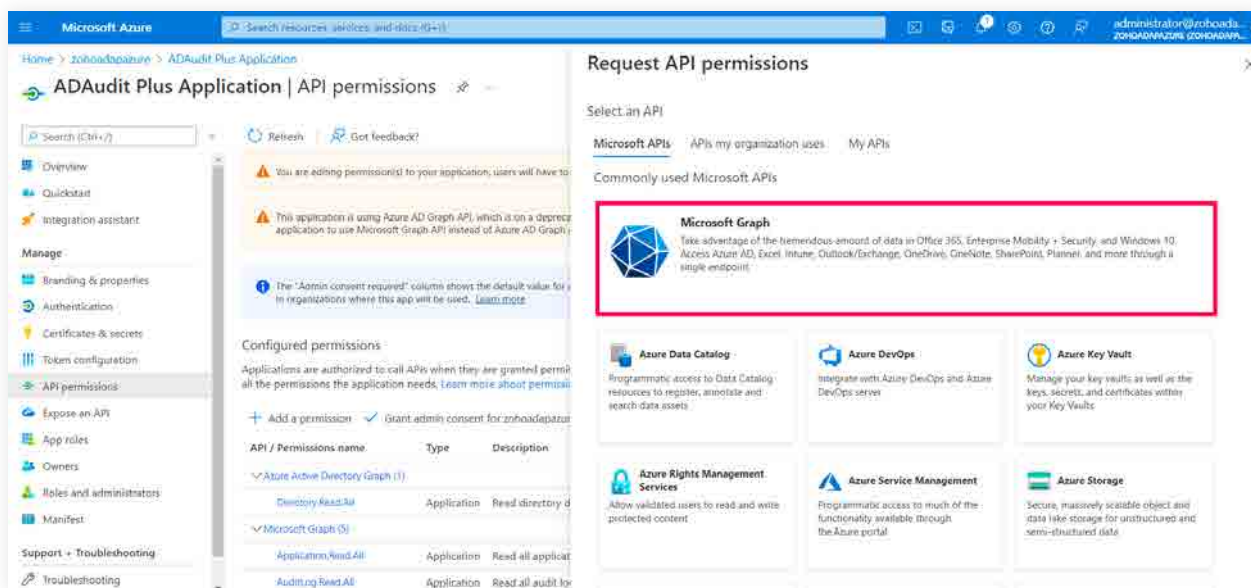
7. In the Request API permissions window, select **Application permissions**, then check the **ActivityFeed.Read** box under ActivityFeed. Select **Add permissions**.



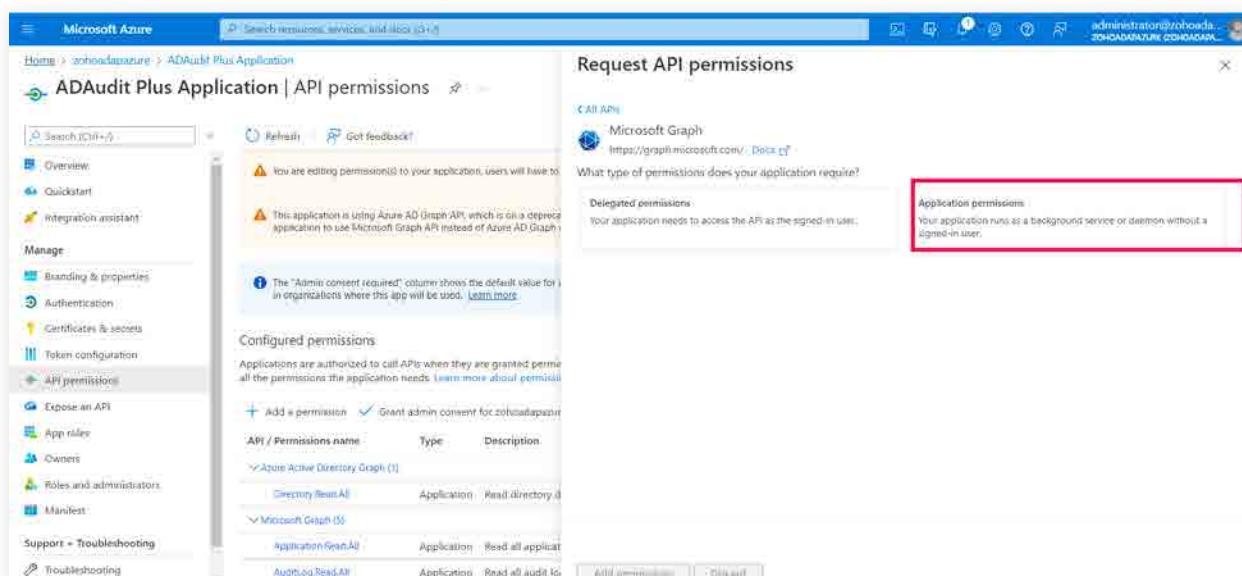
8. Once again, go to **Manage > API permissions > + Add a permission**.



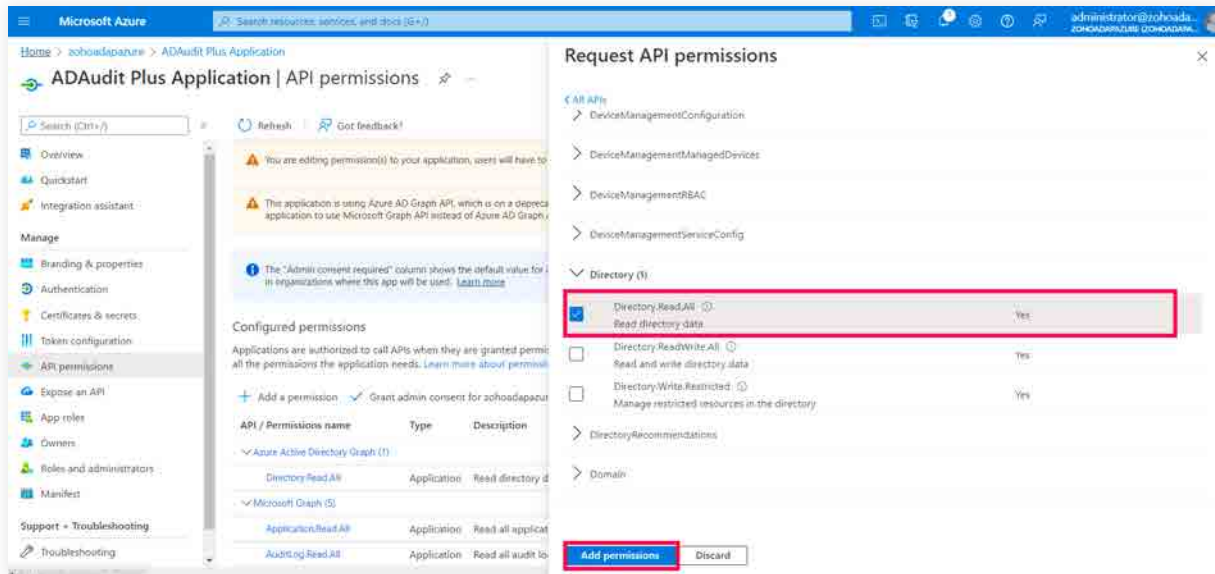
9. Select **Microsoft Graph** in the Request API permissions window.



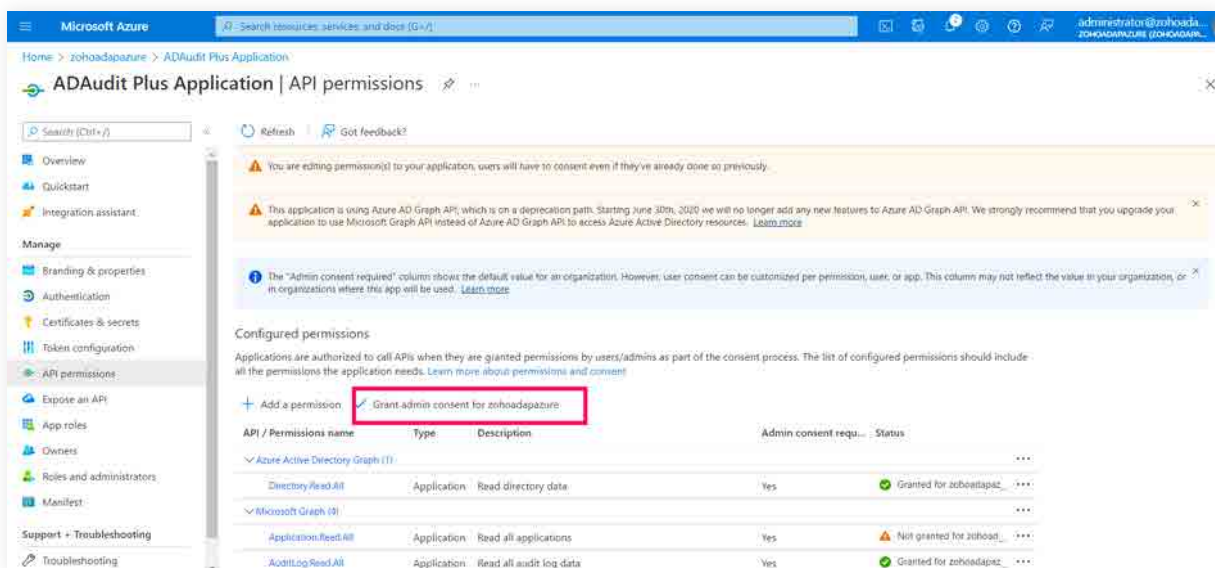
10. Select Application permissions.



11. Check the Directory.Read.All box under Directory. Select Add permissions.



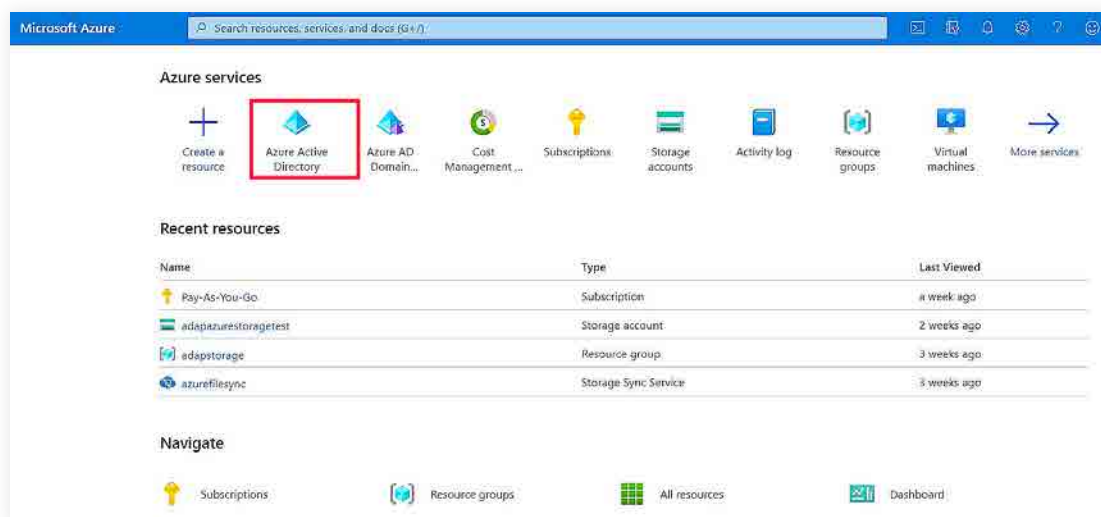
12. Select **Grant admin consent for <tenant name>**.



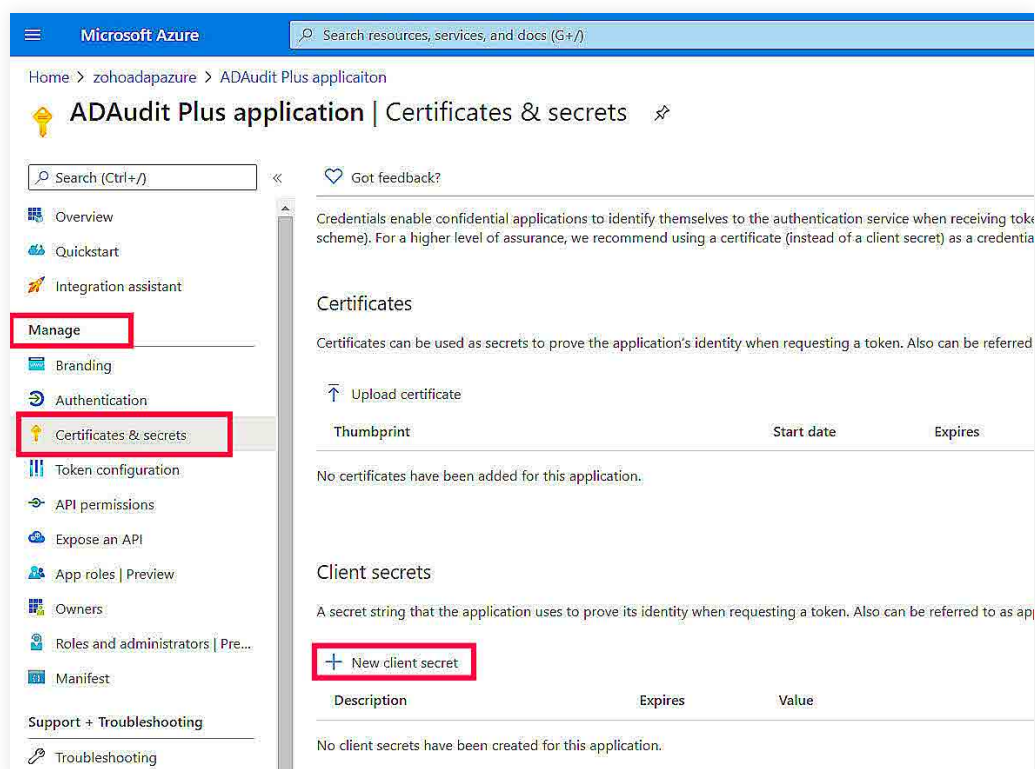
13. Click **Yes**.

Obtain client ID and client secret

1. Go to the [Azure portal](#), and sign in using your Microsoft account.
2. Select **Azure Active Directory** service from the Azure services section.



3. Go to **Manage > Certificates & secrets**.
 - Click **+ New client secret**.
 - Type in the description and the expiration date.
 - Click **Add**.



The screenshot shows the 'Add a client secret' dialog in the Microsoft Azure portal. The dialog has a 'Description' field and an 'Expires' section with three radio button options: 'In 1 year' (selected), 'In 2 years', and 'Never'. Below the dialog is the 'Client secrets' section, which is currently empty, showing a table with headers 'Description', 'Expires', 'Value', and 'ID'. A message states: 'No client secrets have been created for this application.'

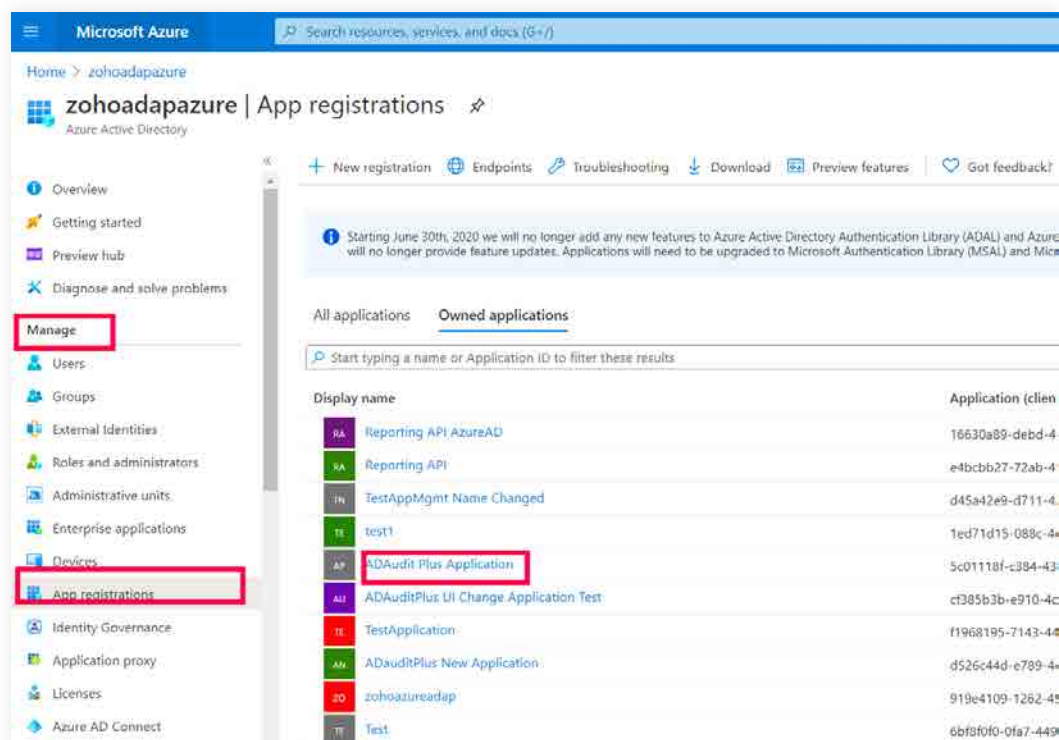
4. Copy the **client secret value** (e.g., 14uClXkHtIVGR3wkCq12341Nd5VtestkkWTyIPrrE=).

The screenshot shows the 'Client secrets' section in the Microsoft Azure portal. A message at the top says: 'Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.' Below this is a table with headers 'Thumbprint', 'Start date', and 'Expires'. The table is currently empty. Below the table is the 'Client secrets' section, which is currently empty, showing a table with headers 'Description', 'Expires', 'Value', and 'ID'. A message states: 'No client secrets have been added for this application.'

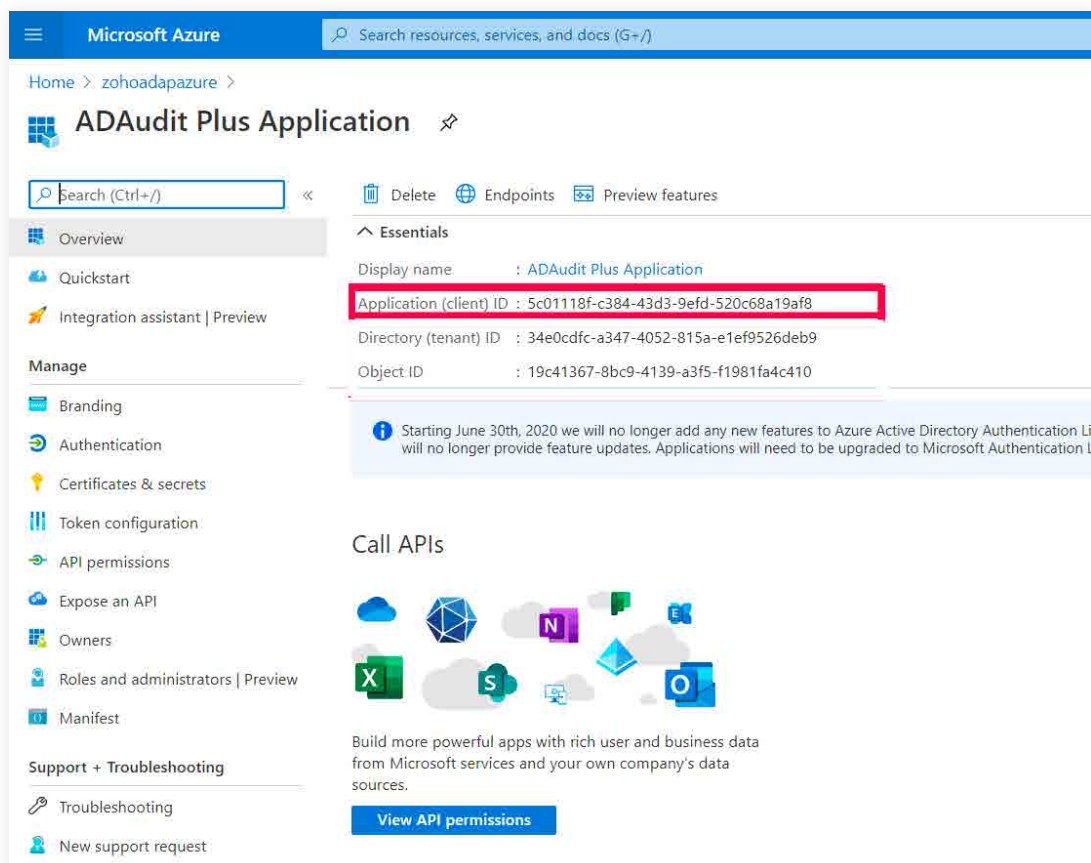
Below the 'Client secrets' section, there is a table with the following data:

Description	Expires	Value
ADAudit Plus application description	11/16/2021	opGY.mZrq_9kpXvh9aLLn~21tdH0~h1JG_

5. Go to **Manage > App registrations**. Select **your application** under Owned applications.

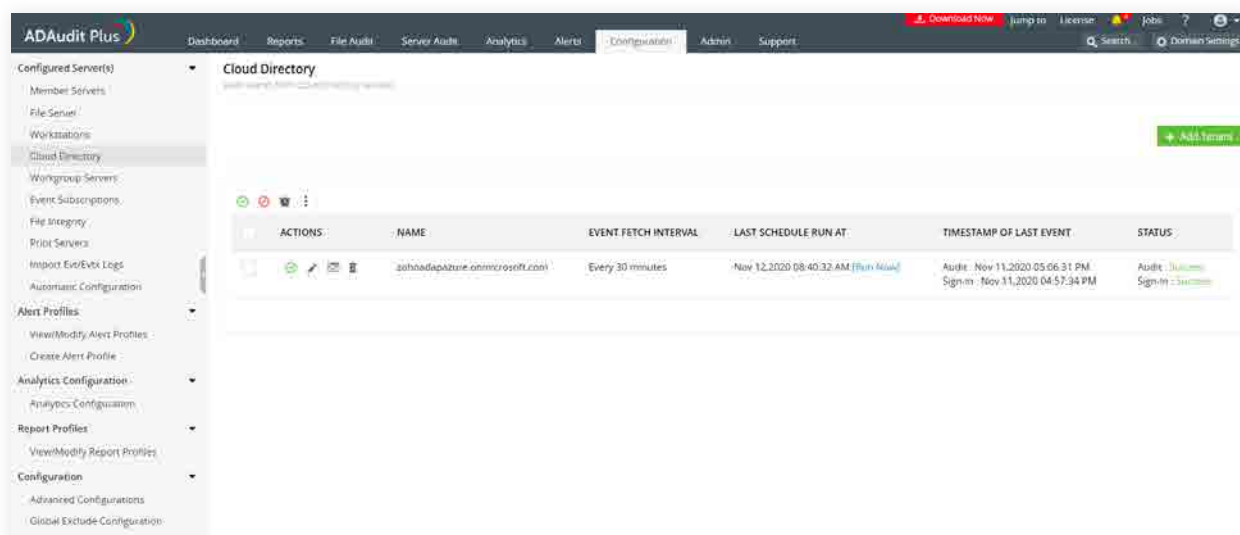


6. Navigate to **Application (client ID)** and click **Copy to clipboard**.

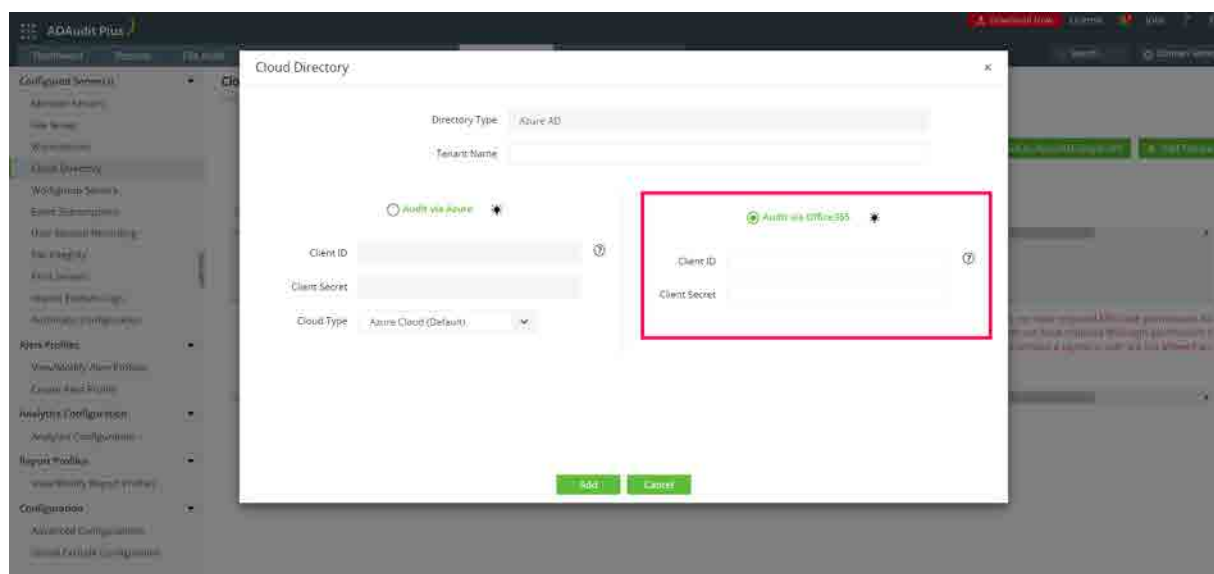


Setting up Azure AD in ADAudit Plus

1. Open the ADAudit Plus web console.
2. Go to **Configuration > Configured Server(s) > Cloud Directory**.



3. Select **+ Add Tenant**.
4. Select **Audit via Office 365**.
5. In the **Cloud Directory** window, enter the **Client ID** and **Client Secret**.



6. Click **Add**.

Privileges required for Office 365 cmdlet configuration

ADAudit Plus uses the below-listed APIs to audit Azure AD.

- Office 365 Management API for all installations after ADAudit Plus build 7050.
- PowerShell cmdlets (unified audit log) for tenants who configured Azure AD via Office 365 before ADAudit Plus build 7050.

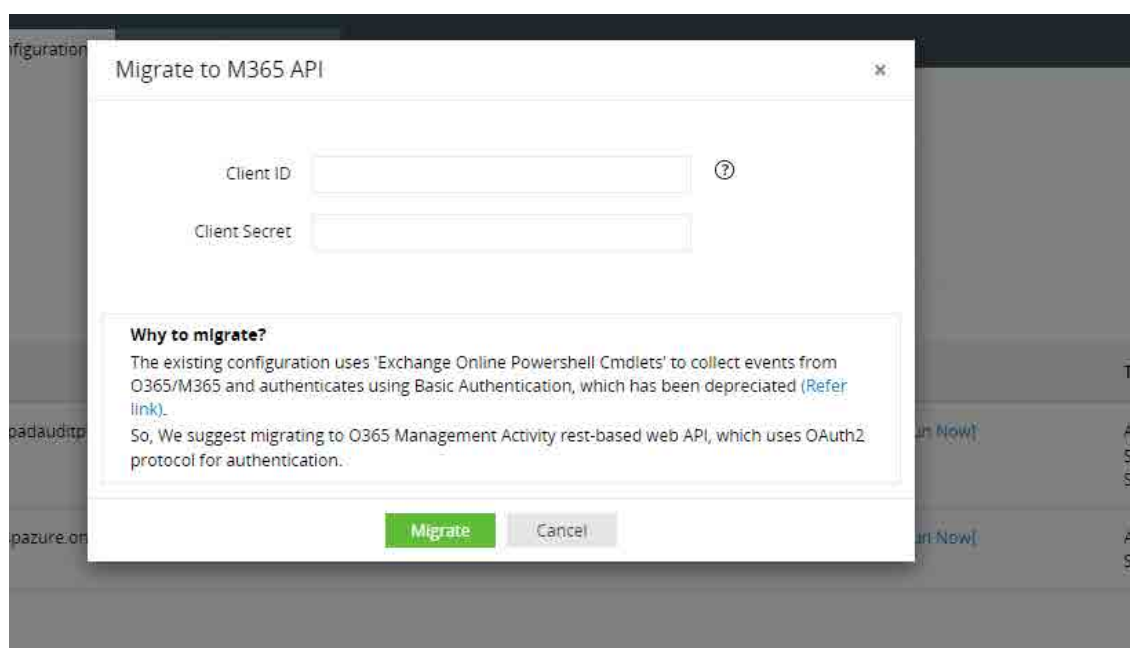
Note: ADAudit Plus strongly recommends using Office 365 Management API to obtain Azure AD events. For tenants still using PowerShell cmdlets, you can update your configuration by migrating O365 cmdlet configuration to Office 365 Management API configuration. You can find the steps to do it here.

Check and migrate O365 cmdlet configuration to M365 API configuration

1. Open the ADAudit Plus web console.
2. Go to **Configuration > Configured Server(s) > Cloud Directory**.
3. Under the Actions column in the report, select the **Migrate** icon.

Note: This is only necessary for tenants who configured Azure AD via O365 before build 7050. This feature will be available once the users upgrade to build 7050 or above.

4. In the *Migrate to M365 API* window that opens, enter the **Client ID** and **Client Secret** generated previously.



5. Click **Migrate**.

If you still want to use O365 cmdlet configuration and you are using an ADAudit Plus build lower than 7050, you can find the privileges required below:

Required role	Permission
Global administrator	Compliance Management (Audit Logs)
	Organization Management (View-Only Audit Logs)

Listed below are the system specifications required:

i. Microsoft .NET Framework 4.0

- To check whether .NET Framework 4.0 is installed:
- Go to **Start > Command Prompt**.
Type in the following query: **reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\full" /v version**.
- Ensure that the version number is 4.0.
If not, download **NET Framework 4.0** from [here](#) and install it.

ii. PowerShell version 3

To check whether PowerShell is installed:

- Go to **Start > Run**.
- Type in **PowerShell**.
- If PowerShell is installed, check for its version number by typing in the following query in the command prompt: **\$PSVersionTable**.
- If PowerShell is not installed or if the existing PowerShell version is below 3, you can install or upgrade to version 3 from [here](#).

iii. Azure AD module for Windows PowerShell

To check whether the Azure AD module is installed:

- Go to **Start > Run**
- Type in **PowerShell**.
- Type in the query **get-module -Name AzureAD**. This will list the module if it's already installed.
In case it's not, install the module by running the PowerShell cmdlet **Install-Module Azure AD**.

Notes:

- Gain a correlated view of your hybrid AD environments by configuring both Azure AD and on-premises AD domain details in ADAudit Plus.
- This Azure AD module is available only in the 64-bit version of Windows.

4. Reporting capabilities of ADAudit Plus

4.1. ADAudit Plus vs. Azure portal

ADAudit Plus	Azure portal
On-premises domain details	
Displays both on-premises and cloud details, such as SID, GUID, and user distinguished name	Only displays details available in the cloud, such as user name and display name
Activity origin	
Generates details on where the activity began, e.g., in the cloud or synced from Windows servers	Does not include details on where the activity began
Retention	
Retains historical data based on the retention period configured by the user	Amount of data stored depends on the license level in Azure (maximum retention duration is 30 days)
Reports	
Analyzes user login details across both on-premises and cloud environments from a single console	Generates only cloud login details in reports

Table 2: A detailed comparison of how auditing via ADAudit Plus differs from auditing via the Azure portal over multiple categories.

4.2. ADAudit Plus vs. Microsoft 365 (using PowerShell cmdlets)

ADAudit Plus	Microsoft 365
On-premises domain details	
Displays both on-premises and cloud details, such as SID, GUID, and user distinguished name	Only displays details available in the cloud, such as user name and display name
Activity origin	
Generates details on where the activity began, e.g., in the cloud or synced from Windows servers	Does not include details on where the activity began
Retention	
Retains historical data based on the retention period configured by the user	Amount of data stored is based on the license level in Microsoft 365 (maximum retention duration is 90 days)
Reports	
Lists user login details across both on-premises and cloud environments from a single console	Generates only cloud login details in reports

Table 3: A detailed comparison of how auditing via ADAudit Plus differs from auditing via Microsoft 365 over multiple categories.

5. Event categories tracked by ADAudit Plus

5.1. Event details

Listed below are the event categories that are monitored by ADAudit Plus.

Azure Active Directory — Application

Azure Active Directory — Device

Azure Active Directory — Directory

Azure Active Directory — Group

Azure Active Directory — Policy

Azure Active Directory — Role

Azure Active Directory — Sign-in

Azure Active Directory — User

Azure Active Directory

6. Log retention settings in Azure AD

It is imperative to retain an adequate amount of historical audit data to meet any compliance or forensic requirements that might arise. The retention period for both Microsoft 365 and Azure AD is based on the user's license level and allows for only a maximum of 90 days. ADAudit Plus, however, provides admins with the option to configure any custom retention period, ensuring a foolproof audit trail.

7. Troubleshooting

Errors and solutions

1. [Failed to add tenants. Check your client secret.](#)
2. [Unable to add tenants due to invalid client ID.](#)
3. [Invalid tenant name.](#)
4. [Insufficient privileges to audit Azure AD.](#)
5. [The Azure AD server is taking too long to respond. Check your network connectivity.](#)
6. [Unable to connect with the Azure AD server due to connection reset.](#)
7. [Unable to connect with the Azure AD server due to trust failure.](#)
8. [Certificate update in progress. Restart the ADAudit Plus service.](#)
9. [The sign-in logons require an Azure AD premium license.](#)
10. [Insufficient privileges when auditing via Office 365.](#)
11. [The configured proxy server is unreachable.](#)
12. [Network unreachable.](#)
13. [Unauthenticated proxy server configured.](#)
14. [Spike in Azure AD event requests.](#)
15. [The event collection is taking too long.](#)
16. [Insufficient privileges to carry out risk detection.](#)
17. [No data available.](#)

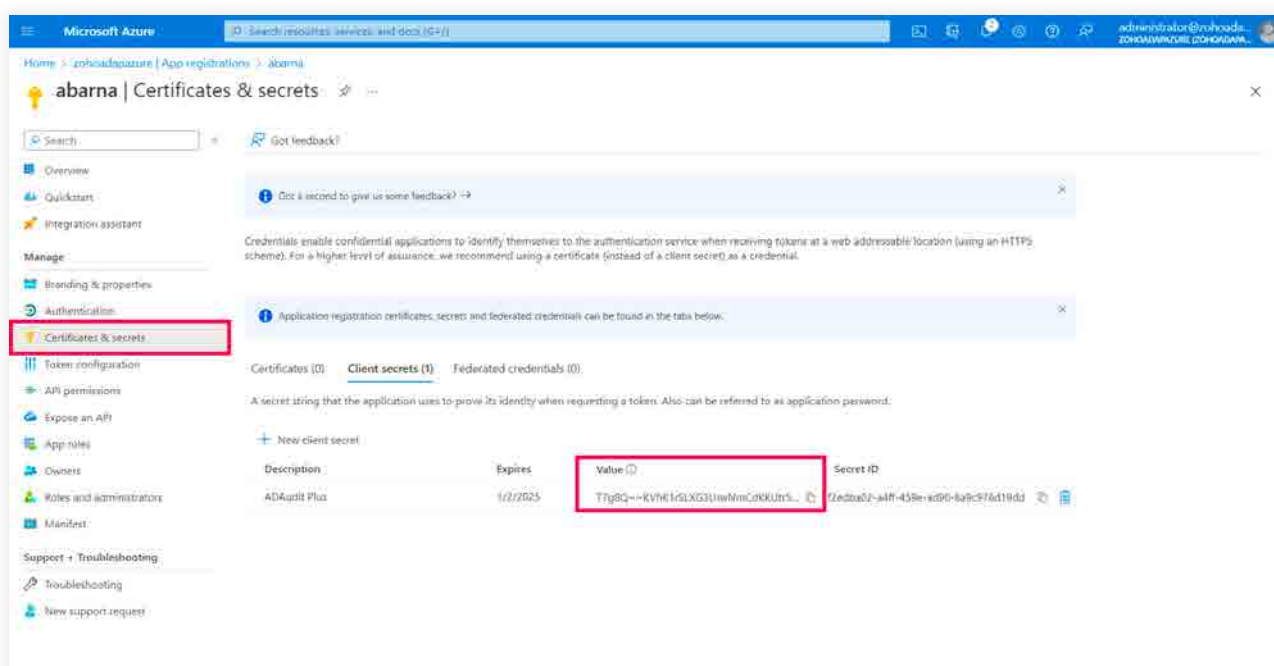
1. Failed to add tenants. Check your client secret.

Issue: Unable to add tenants to configure Azure AD due to invalid client secret.

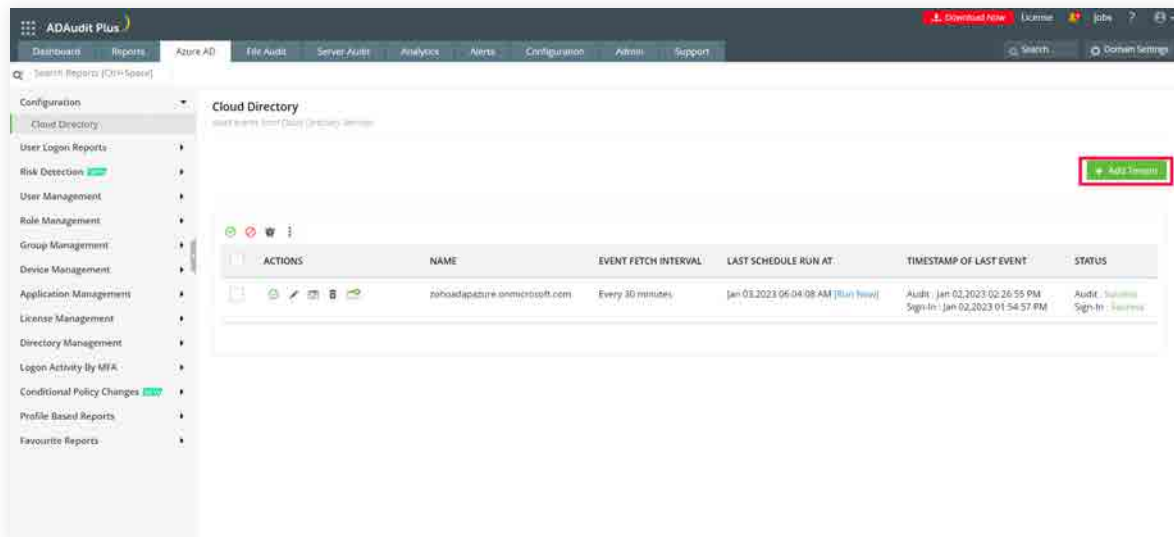
Solution: Client secret values will be available only while it is generated. So, if you have a copy of your current client secret copied elsewhere, you can use it to compare to the value configured in ADAudit Plus. If not, you will have to create a new client secret.

Generate a new client secret by following the steps listed below:

- i. Go to the Azure portal.
- ii. Select the **Azure Active Directory** service from the **Azure services** top pane.
- iii. Go to **Manage > App Registrations**. Select your application under Owned application.
- iv. Go to **Manage > Certificates & secrets**.
- v. Click **+ New client secret**.
- vi. Type in the description. Click Add.
- vii. Copy the client secret value (e.g., "14uClLxkHtIVGR3wkCq12341Nd5VtestkkWTyIPrrE=")



- viii. Now open the ADAudit Plus console.
- ix. Navigate to **Azure AD > Configuration > Cloud Directory**.



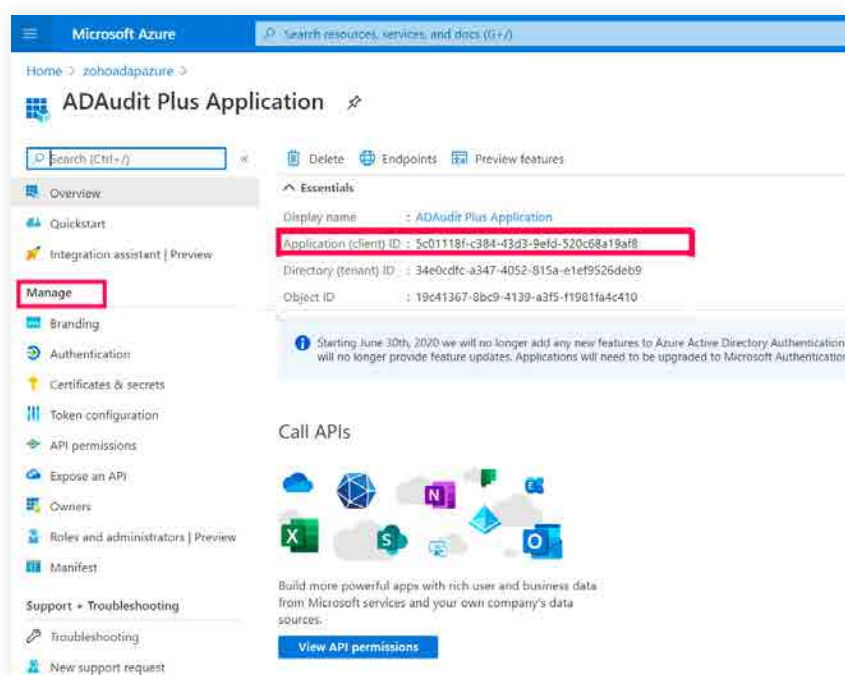
- x. Click **+ Add Tenant** icon at the top-right corner.
- xi. Input the tenant name, client ID, and client secret value.
- xiii. Click **Save**.

2. Unable to add tenants due to invalid client ID

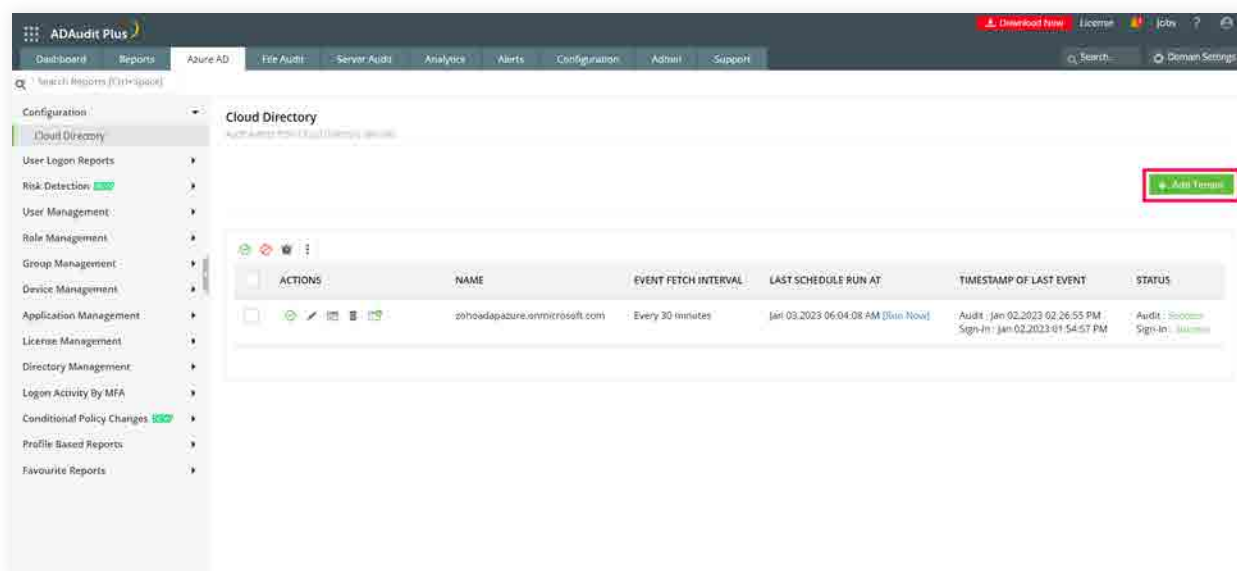
Issue: Unable to add tenants to configure Azure AD due to invalid client ID.

Solution: Check if you have entered the correct client ID by following the steps listed below:

- i. Go to the Azure portal.
- ii. Select the **Azure Active Directory** service from the **Azure services** top pane.
- iii. Go to **Manage > App registrations**. Select your application under **Owned applications**.
- iv. Navigate to **Application (client ID)** and click **Copy to clipboard**.



- v. Now open the ADAudit Plus console.
- vi. Navigate to **Azure AD > Configuration > Cloud Directory**.

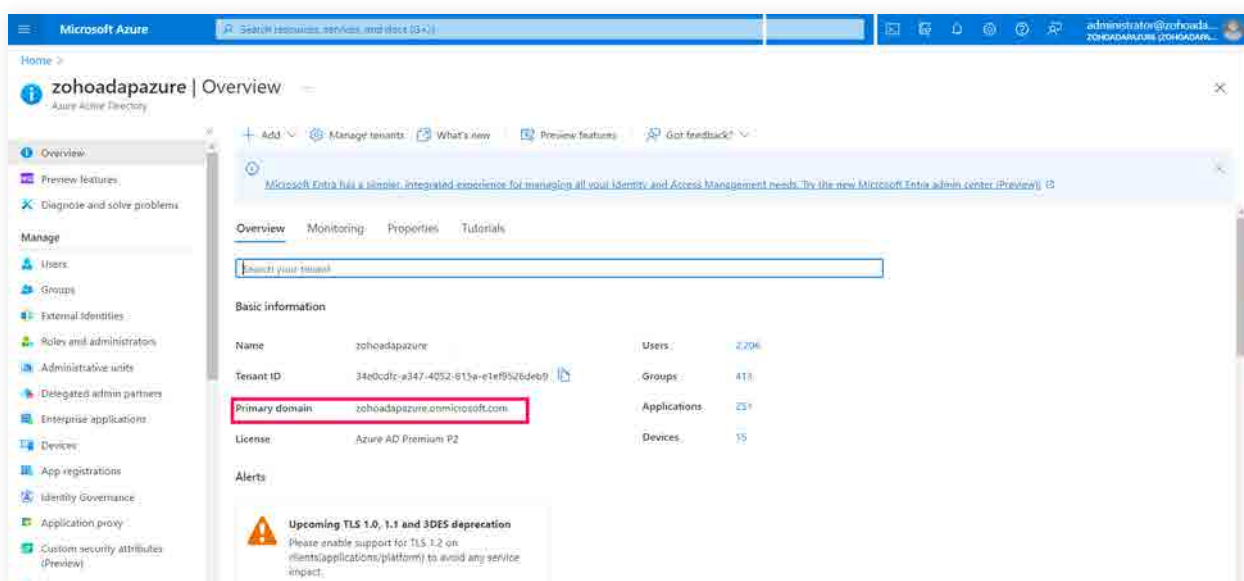


- vii. Click **+ Add Tenant** icon at the top-right corner.
- viii. Input the tenant name, client ID, and client secret values.
- ix. Click **Save**.

3. Invalid tenant name

Issue: Unable to add tenant due to invalid tenant name.

Solution: Check if you have entered the correct tenant name by following the steps listed below:



- i. Go to the Azure portal.
- ii. Select the **Azure Active Directory** service from the **Azure services** top pane.
- iii. Go to **Overview** in the left pane. Copy the tenant name.
- iv. Now open the ADAudit Plus console.
- v. Navigate to **Azure AD > Configuration > Cloud Directory**.
- vi. Click **+Add Tenant** at the top-right corner.
- vii. Type in the correct tenant name, client ID, and client secret values.
- viii. Click **Save**.

4. Insufficient privileges to audit Azure AD

Issue: The application does not have the necessary privileges required to audit the cloud directory.

Solution: Grant the minimum required permissions for application created to audit Azure AD using the steps listed [on this page](#).

5. The Azure AD server is taking too long to respond. Check your network connectivity

Issue: There is a connectivity issue between the ADAudit Plus server and Azure AD server.

Solution: Check if there is a stable and reliable internet connection with a speed of 20Mbps or over.

If there is proxy configured in the machine where ADAudit Plus is installed, then configure proxy setting in ADAudit Plus too, using these steps:

- In ADAudit Plus web console, go to **Admin > Connection > Proxy**.
- Check the **Proxy Server Settings** checkbox.
- Type in the proxy server details.
- Click **Save**.

6. Unable to connect with the Azure AD server due to connection reset.

Issue: A firewall could be restricting ADAudit Plus from connecting with the Azure AD server.

Solution: If you are using a firewall to secure your network, kindly ensure that the domains listed below are added to the exemption list.

<https://login.microsoftonline.com>

<https://outlook.office365.com>

<https://graph.windows.net>

<https://graph.microsoft.com>

<https://manage.office.com>

If you do not use a firewall, or if the issue persists even after upgrading to the latest build, contact [support](#).

7. Unable to connect with the Azure AD server due to trust failure.

Issue: A firewall could be restricting ADAudit Plus from connecting with the Azure AD server.

Solution: If you are using a firewall to secure your network, kindly ensure that the domains listed below are added to the exemption list.

<https://login.microsoftonline.com>

<https://outlook.office365.com>

<https://graph.windows.net>

<https://graph.microsoft.com>

<https://manage.office.com>

If you do not use a firewall or if the issue persists even after upgrading to the latest build, contact [support](#).

8. Certificate update in progress. Restart ADAudit Plus service

Issue: The updated Azure certificate is missing from the ADAudit Plus trust store.

Solution: Restart the ADAudit Plus service to reflect the already updated certificate in the ADAudit Plus trust store.

Note: The required certificate will be automatically updated to the ADAudit Plus trust store.

9. The sign-in logons require Azure AD premium license

Issue: Details of sign-ins can be obtained only if the tenant has an Azure Active Directory P1 or P2 license.

Solution: Upgrade your Azure license. For more details [here](#).

10. Insufficient privileges when auditing via Office 365

Issue: The application configured for O365 API does not have the necessary privileges required to audit the cloud directory.

Solution: Grant the minimum required permissions for application created to audit Azure AD using the steps listed on this [page](#).

11. The configured proxy server is unreachable

Issue: The configured proxy server is not running.

Solution: Check the proxy server's running status. If it's running, configure it in ADAudit Plus' proxy setting.

If the issue persists contact [support](#).

12. Network unreachable

Issue: The server that ADAudit Plus is installed on can't connect to the internet.

Solution: Check the server's internet connection and provide internet connectivity if you haven't done so already.

Note: The required certificate will be automatically updated to the ADAudit Plus trust store.

13. Unauthenticated proxy server configured

Issue: Although an authenticated proxy server is available, an unauthenticated setup is configured in the ADAudit Plus console.

Solution: Configure the right username and password on the ADAudit Plus proxy setting page, using these steps:

- In ADAudit Plus web console, go to **Admin > Connection > Proxy**.
- Check the **Proxy Server Settings** checkbox.
- Type in the proxy server details.
- Click **Save**.

14. Spike in Azure AD event requests

Issue: There is a sudden spike in the number of requests to Azure AD.

Solution: The issue will be fixed automatically when you upgrade to build 7080 or above.

Find the service pack to upgrade to build 7080 [on this page](#).

15. The event collection is taking too long

Issue: The event fetch has been running for a long time.

Solution: Click run-now. If it keeps throwing the same error, contact [support](#).

16. Insufficient privileges to carry out risk detection

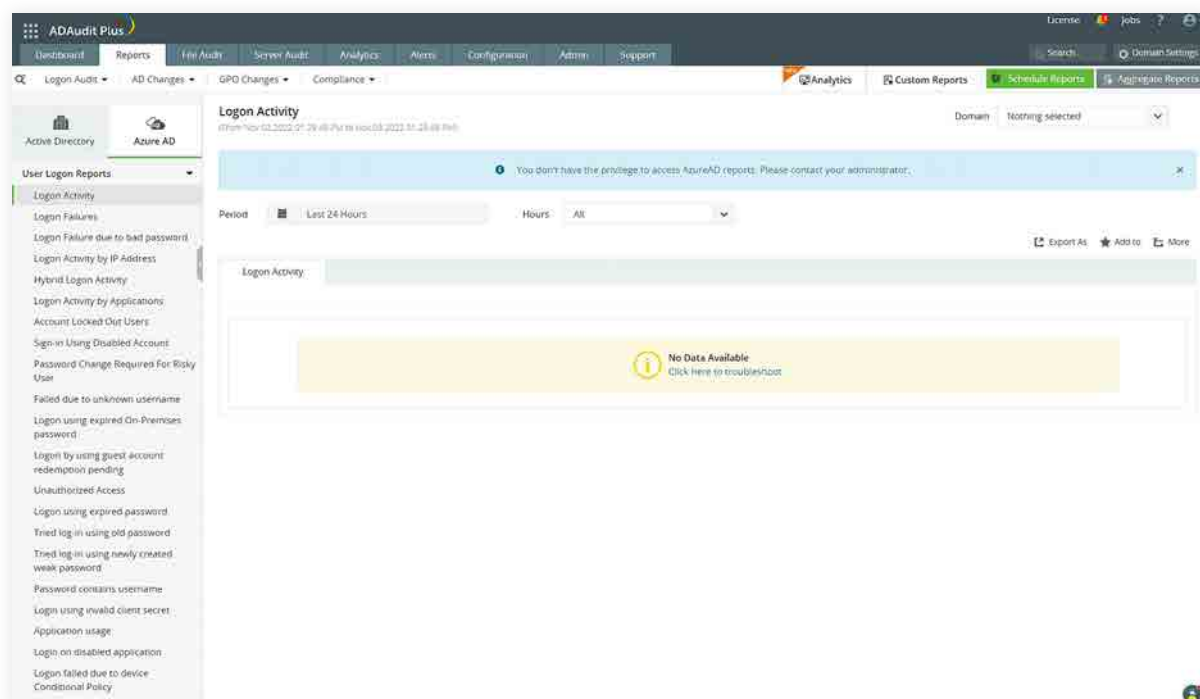
Issue: The Azure AD premium license does not have the required privileges to analyze risky sign-in activities.

Solution: Find the minimum required permissions for application created to populate information about risky sign-in action in Azure AD using the steps listed [on this page](#).

17. No data available

Issue: Data unavailable for the reports under Azure AD

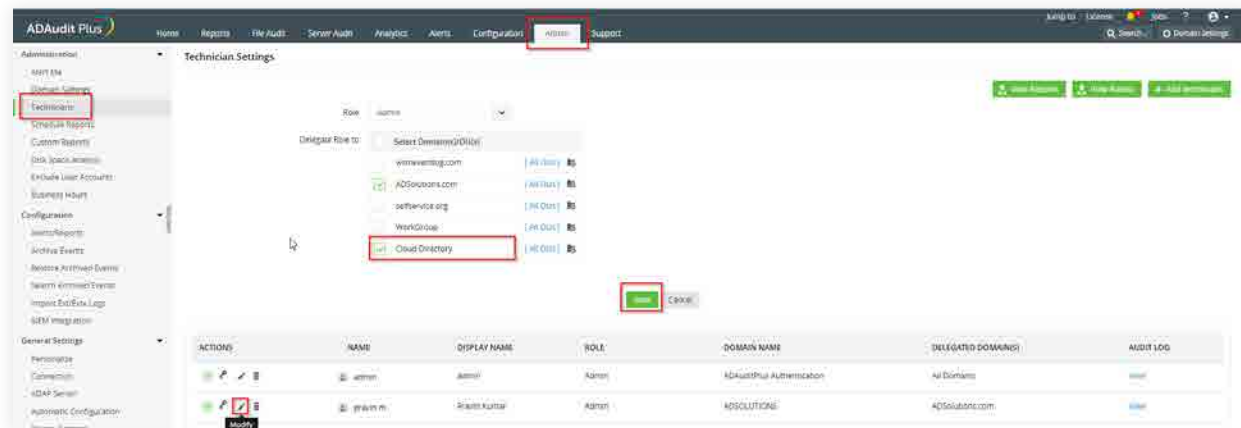
Solution: This issue could stem from multiple factors. One of which is insufficient privileges, i.e., the account used to logon to ADAudit Plus does not have necessary privileges to audit Azure. In such cases, there will be an in-product notification as shown in the screenshot below.



To resolve this, check if the account you have used to logon has privileges to view Cloud Directory reports using the steps below:

- Open ADAudit Plus web console.
- Go to **Admin > Technicians**.
- Click the **Modify** icon under the Action column next to the name of the user account you have used to logon.
- Check **Cloud Directory** under Delegate Role to list.

Now verify if you can view the Azure AD reports by logging on using that user account.



If you have the necessary privileges and are still not able to populate any reports under the Cloud Directory, [contact support](#).

About ADAudit Plus

ManageEngine ADAudit Plus is an IT security and compliance solution. With over 200 event-specific reports and real-time email alerts, it provides in-depth knowledge about changes effected to both the content and configuration of Active Directory, Azure AD and Windows servers. Additionally it also provides thorough access intelligence for workstations and file servers (including NetApp and EMC).

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit: <https://www.manageengine.com/products/active-directory-audit/>

\$ Get Quote

Download