Table of contents

1. Introduction ........................................................................................................... 1

2. Comparing the methods for configuring Azure AD ................................................. 2

3. Configuring Azure AD in ADAudit Plus ................................................................. 2

   3.1 Using an Azure AD Premium license ................................................................. 2

      3.1.1 Privileges required for configuration ......................................................... 3

      3.1.2 Azure AD app creation ............................................................................... 3

      3.1.3 Setting up Azure AD in ADAudit Plus ......................................................... 11

   3.2 Using a Microsoft 365/Office 365 license .......................................................... 12

      3.2.1 Privileges required for configuration ......................................................... 12

      3.2.2 System requirements ............................................................................... 13

      3.2.3 Setting up Azure AD in ADAudit Plus ......................................................... 14

4. Reporting capabilities of ADAudit Plus ................................................................. 15

   4.1 ADAudit Plus vs. Azure portal ........................................................................... 15

   4.2 ADAudit Plus vs. PowerShell cmdlets .............................................................. 16

5. Event categories tracked by ADAudit Plus .......................................................... 16

   5.1 Event details ...................................................................................................... 16

6. Log retention settings in Azure AD ........................................................................ 17

7. Troubleshooting ...................................................................................................... 17
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

Url:

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

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Azure</th>
<th>Microsoft 365 or Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>MFA details</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>Group-based license change</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>Application display name</td>
<td>Possible</td>
<td>Possible by using the Azure AD module</td>
</tr>
<tr>
<td>Modified properties, along with their new and old values</td>
<td>Possible</td>
<td>Not possible with basic edition of Microsoft 365 or Office 365 E1 licensing</td>
</tr>
</tbody>
</table>

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

3. Configuring Azure AD in ADAudit Plus

Url:

**3.1 Using an Azure AD Premium license**

You can choose to audit your Azure AD environment using an Azure AD Premium license. In this method, ADAudit Plus uses the Azure reporting API to obtain events from Azure AD.
3.1.1 Privileges required for configuration

Grant the following privileges depending on the API you need access to:

<table>
<thead>
<tr>
<th>API</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Azure Active Directory</td>
<td>Read directory data</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Read all audit log data</td>
</tr>
</tbody>
</table>

3.1.2 Azure AD app creation

Here are the steps to create an application in Azure AD:

1. Register an application.
2. Provide the required minimum privileges.
3. Obtain your application’s client secret.
4. Collect and analyze configuration settings.

1. Register an application

   i. Go to the Azure portal by clicking here, and sign in using your Microsoft account.

   ii. Select the Azure Active Directory service from the Azure services top pane.

   iii. Go to Manage > App registrations > New registrations to open the Register an application window.
iv Enter the application name, e.g., “ADAudit Plus application”.

v Ensure that **Accounts in this organizational directory only (zohoadapazure only - Single tenant)** is selected under **Supported account types**.

vi Click Register.
2. Provide the required minimum privileges

i. Go to the Azure portal by clicking here, and sign in using your Microsoft account.

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**.

iii. Go to **Manage > API permissions** and select **+ Add a permission** to open the Request API permissions window.
Go to Microsoft Graph > Application permissions.
In the Request API permissions window, select **Directory > Directory.Read.All**.

Select **Add permissions**.

Click **Yes** when prompted if you need to Grant Admin Consent for tenantname.
3. Obtain your application's client secret

i. Go to the Azure portal by clicking here, and sign in using your Microsoft account.

ii. Select the Azure Active Directory service from the Azure services top pane.

iii. Go to Manage > Certificates & secrets.

   - Click + New client secret.
   - Type in the description and the expiration date.
   - Click Add.
Copy the client secret value (e.g., "14uCIxkHtIVGR3wkCq12341Nd5VtestkkWTylPrrE=").
4. Collect and analyze configuration settings

i. Go to the Azure portal by clicking here, and sign in using your Microsoft account.

ii. Select the **Azure Active Directory** service from the **Azure services** top pane.

![Azure portal screenshot](image)

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

![App registrations screenshot](image)

iv. Navigate to **Application (client ID)** and click **Copy to clipboard**.
3.1.3 Setting up Azure AD in ADAudit Plus

- Open the ADAudit Plus web console.
- Go to Configuration > Configured Server(s) > Cloud Directory.
- Select + Add Tenant in the top-right corner.
  
- Select Audit via Azure.
- In the Cloud Directory window, type in the Tenant Name, Client ID, and Client Secret.
Click Add.

Url:

3.2 Using a Microsoft 365/Office 365 license

You can choose to audit your Azure AD environment using a Microsoft 365/Office 365 license. In this method, ADAudit Plus uses PowerShell cmdlets (unified audit log) to get events from Azure AD.

3.2.1 Privileges required for configuration

Grant the following privileges for the smooth functioning of ADAudit Plus:

<table>
<thead>
<tr>
<th>Required role</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global administrator</td>
<td>Compliance Management (Audit Logs)</td>
</tr>
<tr>
<td></td>
<td>Organization Management (View-Only Audit Logs)</td>
</tr>
</tbody>
</table>
3.2.2 System requirements

Listed below are the system specifications required for ADAudit Plus.

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 it’s not, download and install .NET Framework 4.0 from [here](#).

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:

i  Gain a correlated view of your hybrid AD environments by configuring both Azure AD and on-premises AD domain details in ADAudit Plus.

ii  This Azure AD module is available only in the 64-bit version of Windows.
3.2.3 Setting up Azure AD in ADAudit Plus

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

- Select + Add Tenant.
- Select Audit via Office 365.
- In the Cloud Directory window, type in the Tenant Name, Username, and App Password.

- Click Add.
4. Reporting capabilities of ADAudit Plus


4.1 ADAudit Plus vs. Azure portal

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

*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/Office 365 (using PowerShell cmdlets)

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

Table 3: A detailed comparison of how auditing via ADAudit Plus differs from auditing via Microsoft 365/Office 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
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/Office 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

Understand and resolve the most common issues faced while auditing Azure using ADAudit Plus:


Error messages and solutions

- **Connection refused: connect**
  - **Issue:** The proxy server is not running.
  - **Solution:** Check the proxy server's running status. If it's running, configure it in ADAudit Plus' proxy setting.

- **Network is unreachable: connect**
  - **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.

- **Unable to tunnel through proxy. Proxy returns "HTTP/1.1 407 Proxy Authentication Required."**
  - **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.

- **This request is throttled. Please try again after some time. CorrelationID: 185ff810-78f4-401f-a322-68a4e2ef41bb**
  - **Issue:** There is a sudden spike in the number of requests to Azure AD.
  - **Solution:** The issue will be fixed automatically during the next event fetch schedule. There will be no loss of data due to this error. If you need to suppress the error message, run the query below and restart the ADAudit Plus service.
update clousystemparams set param_value='This request is throttled. Please try again after some time' where param_name='DISABLE_ALERT_FOR_STATUS'

Token not found: token is either invalid or expired
Issue: The event fetch has been running for a long time.
Solution: Click run-now. If it keeps throwing the same error, contact support.

- Invalid_client.
  Issue: ADAudit Plus is trying to fetch events from the cloud directory via a deleted application.
  Solution: Check the status of the application's availability in Azure AD. If the application is available, contact support.

- Provisioning layer initialization failed: The domain controller 'xxxx.xxx.com' is not available for use at the moment. Please try again later.
  Issue: The domain controller is not available in the cloud directory when ADAudit Plus tries to fetch event data.
  Solution: Wait till the next event fetch schedule for the issue to resolve itself. If it doesn't, contact support.

  Issue: ADAudit Plus is unable to find the Azure AD certificate.
  Solution: To resolve the issue:
  Step 1: Export the Azure AD certificate from this link.
  Step 2: Go to PRODUCT_HOME\jre\lib\security\cacerts.
  Step 3: Import the exported certificate from Step 1 in cacerts using the command below:
  keytool -import -alias example -keystore PRODUCT_HOME\lib\security\cacerts-file example.cer
  Password: changeit
  Step 4: Restart the ADAudit Plus service from services.msc snap.in.

- authentication_requestfromnonpremiumtenantorb2ctenant
  Issue: The configured cloud directory does not have an Azure AD Premium license.
  Solution: Without the Azure AD Premium license, it is impossible to get sign-in activities from Azure. If you have a Microsoft 365/Office 365 license, we can audit Azure using that.

To suppress the alert message, run the query below and restart the ADAudit Plus service:
update clousystemparams set param_value='Premium' where the param_name = 'DISABLE ALERT FOR STATUS'
• **Unable to Connect Server**  
   **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.  
   To suppress the alert message, run the query below and restart the ADAudit Plus service:  
   ```sql  
   update clousystemparams set param_value='Premium' where the param_name ="DISABLE_ALERT_FOR_STATUS"  
   ```

• **Authentication_ApplicationHasNoDirectoryReadAccess**  
   **Issue:** The application created in Azure AD does not have the necessary privileges to read directory data.  
   **Solution:** Provide the necessary permission to read directory data from Azure AD and create an Azure AD application using this link.

• **An error caused a change in the current set of domain controllers**  
   **Issue:** The domain controller is not available in the cloud directory when ADAudit Plus tries to fetch event data.  
   **Solution:** Wait till the next event fetch schedule for the issue to resolve itself.  
   If it doesn't, 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/