Integrating Azure with Authomize

Azure can be integrated with Authomize so that Authomize will be able to analyze identity and access information held on Azure. Information such as users, groups, roles and applications are extracted once and updated regularly thereafter.

Note: When Azure is integrated, Azure AD and Microsoft Office 365/SharePoint/OneDrive are also integrated.

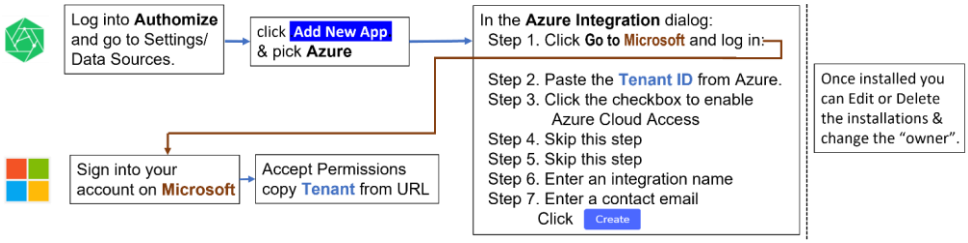
Commented [YI1]: @Amir Avitzur I would remove the word crucial, since users can still get value from Authomize without this data

Commented [AA2R1]: done

Commented [YI3]: The guide should talk about Azure AD, O365 and Share point (as you've done in section #7)

Commented [AA4R3]: done

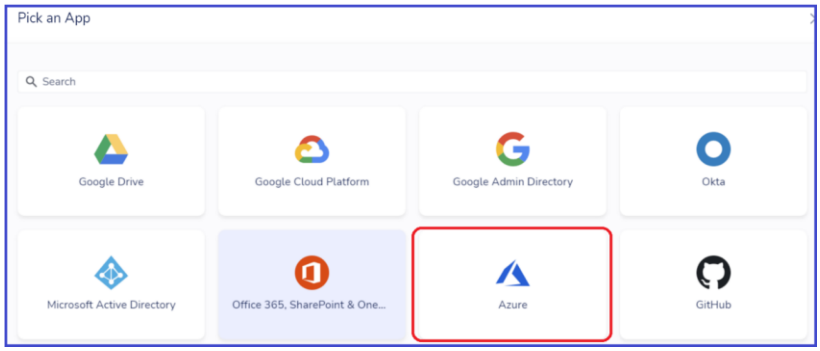
Azure integration workflow



Integrating Azure with Authomize

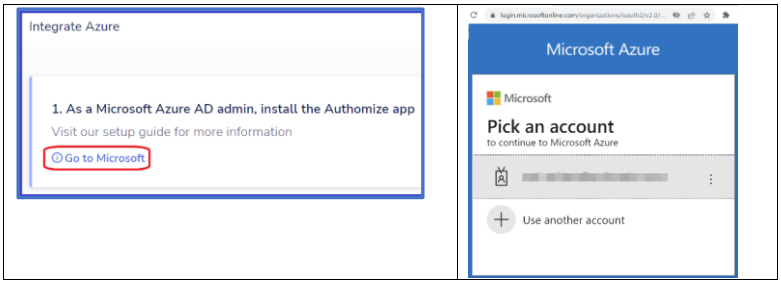
1. Log into **Authomize**
2. Go to Settings/Data Sources and click **Add New App**.

3. Select ***Azure*** or ***Microsoft Active Directory*** or ***Office 365, SharePoint & OneDrive*** to open the integration dialog.

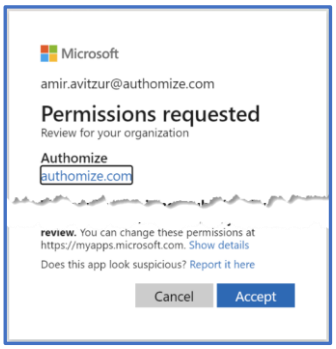


4. In the ***Integrate Azure*** (or ***Integrate MS Active Directory*** or Integrate ***Office 365 …***) dialog:

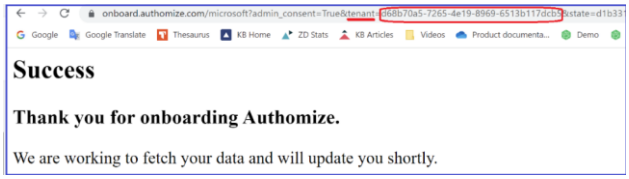
Step 1. Click **Go to Microsoft** and log in.



Have a look through the permission needed by Authomize. If you agree click **Accept**.

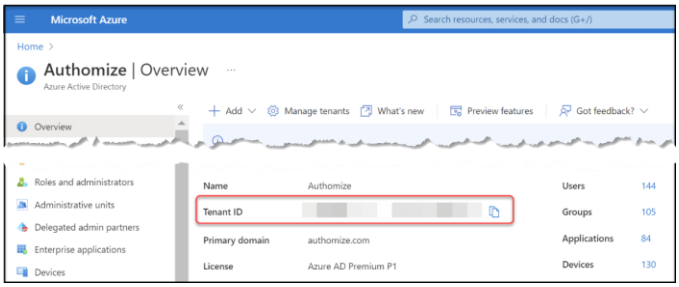


You will see this, if all goes well:



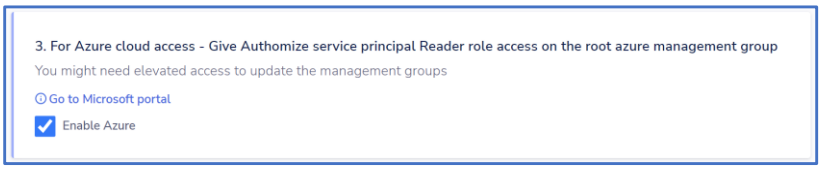
Copy the **tenant** from the URL (see the Appendix for more details).

Alternatively, copy the Tenant ID from the Authomize|Overview page in Microsoft Azure

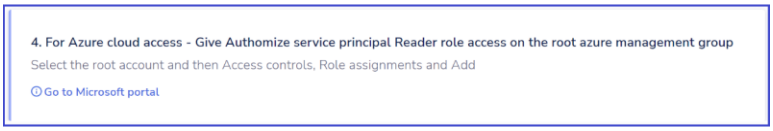


Step 2. Paste the **Tenant ID** from Azure.

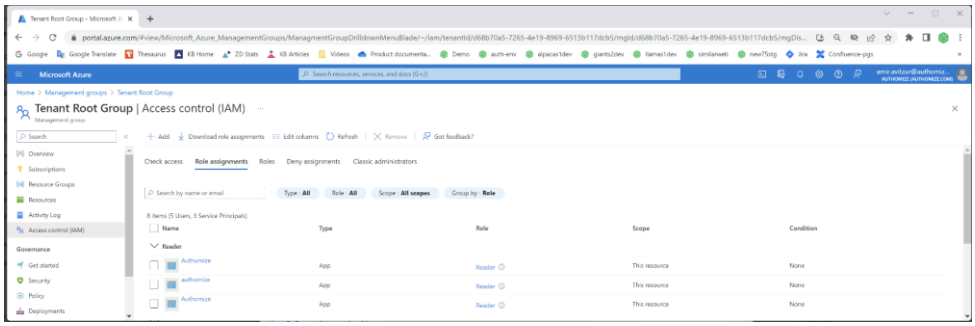
Step 3. Click the checkbox to give Authomize a principal Reader role on the root Azure management group. (If not checked, very limited data will be collected).



Step 4. Click **Go to Microsoft Portal**. To confirm that Authomize is set up in a Reader Role.



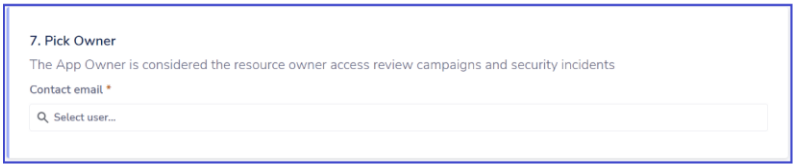
For step-by-step instructions, see Appendix B: Setting up a reader role.



Step 5. Skip this step. There is no need to check *Allow Authomize to update access policies.*

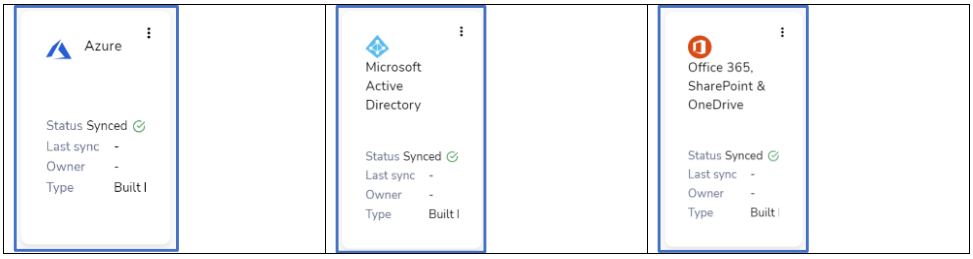
Step 6. Enter an integration name

Step 7. Enter a contact email



Click **Create**

5. Wait for the integration to finish.
   When Azure, or one of the other connectors, are integrated you will see three new entries in the Connected Apps list.



What data is collected

Azure	Microsoft Active Directory	Office 365
• **Application** • **Group** • **Virtual Machine**	• **Application** • **Drive** • **Domain** • **Group** • **Account** • **User** • **Account** • **Integration**	• **Files** • **Folders** • **Drives** **SharePoint** • **Group** • **User** • **Link** **OneDrive** • **Package** • **Resource** • **Account** • **User** • **Group**

Commented [YI5]: @Amir Avitzur need to update to OneLogin

Commented [YI6]: @Amir Avitzur - that's the data we collect: Best Email
City
Country
Department
Division
Employee number
First name
fullName1
Display name
Employee ID
Job Title
lastName
Location
State
Status
supervisor
supervisorId
terminationDate
workEmail

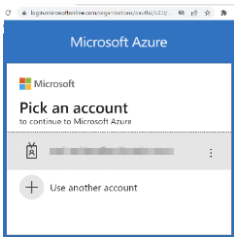
Commented [AA7R6]: Done

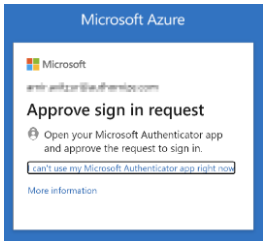
Commented [YI8]: @Amir Avitzur let's divide this section for 3: each per each integration.
For Azure we have much more data: let's add a section for "Cloud resources" and add : Virtual machine, storage accounts, data bases, etc...

Commented [AA9R8]: done

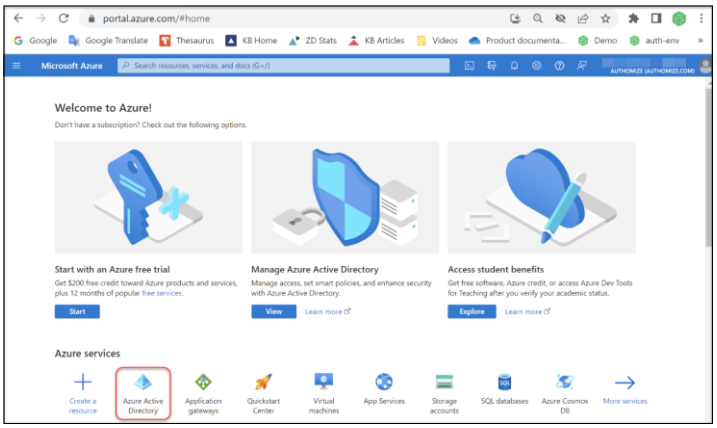
Appendix A: Getting the Tenant ID from Azure

1. Log into portal.azure.com as an admin.:

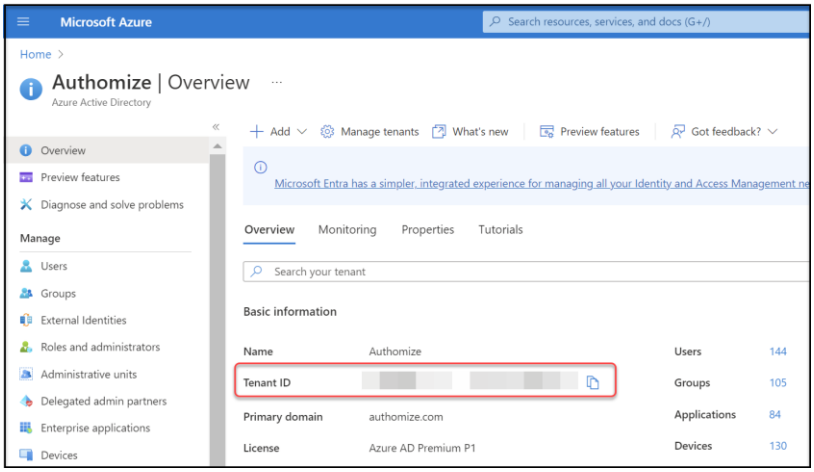




2. Click **Azure Active Directory**.

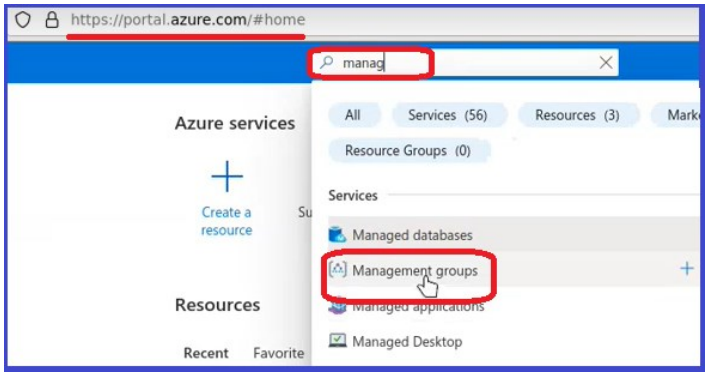


3. On the **Authomize|Overview** page, copy the **Tennant ID.**

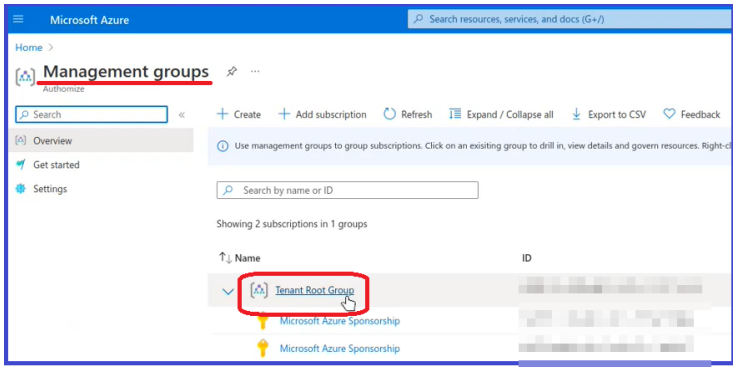


Appendix B: Setting up a reader role

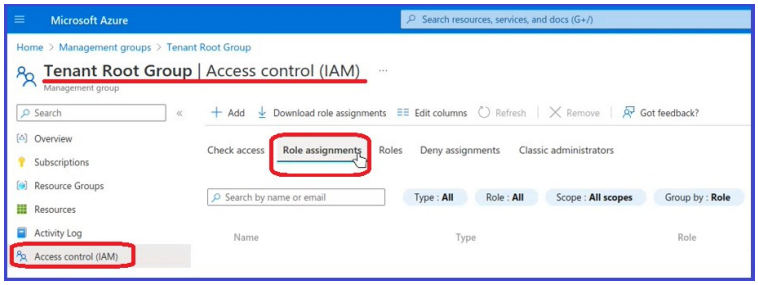
1. Log into Azure.
2. Search for ***Management groups*** and click it when found.



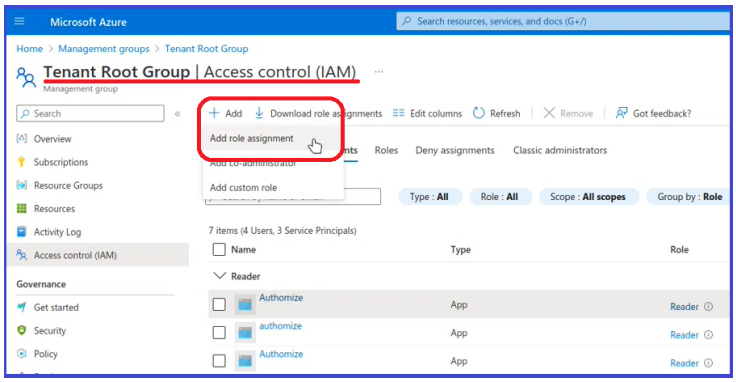
3. In Management groups click ***Tenant Root Group***.



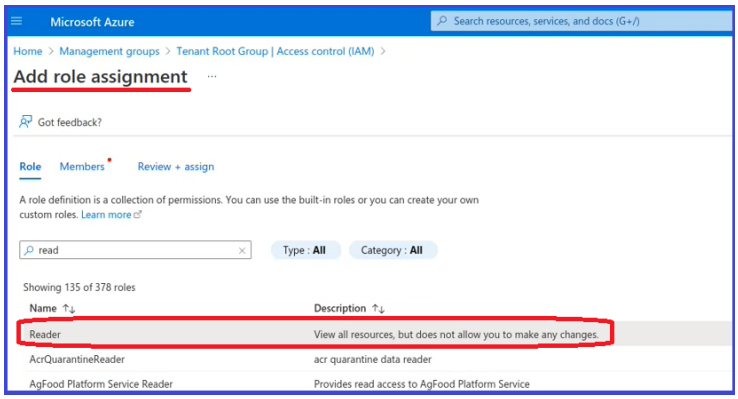
4. In the Tenant Root Group, click Access Control (IAM) in the menu, then click to open the ***Role assignments***.



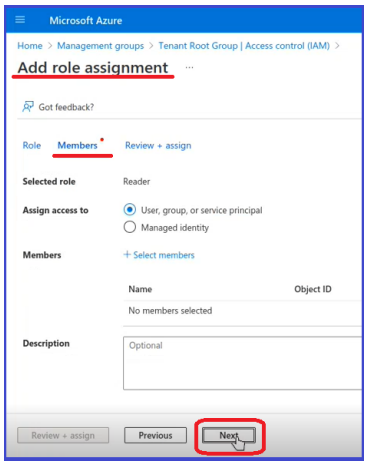
5. In the Tenant Root Group|Access control|Role assignments, click **+** to add a new role assignment.



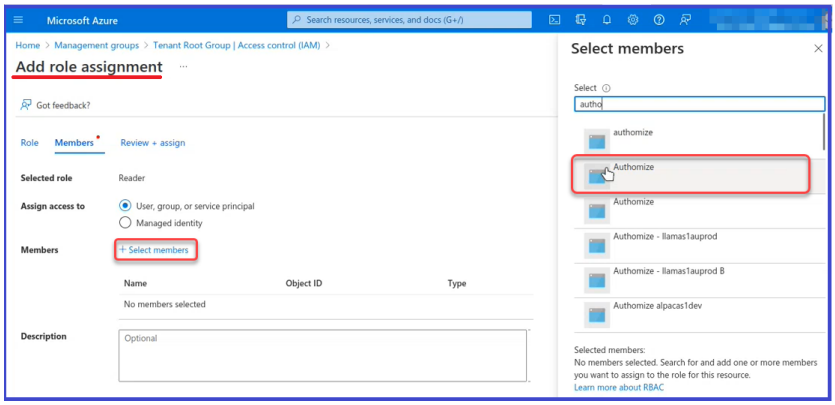
6. In the Add role assignment dialog | Role page, click **Reader**.



7. In the Add role assignment dialog | Members page, click the **Next** button.



8. In the Add role assignment dialog Click ***+ Select members***.
9. Select Authomize from the **Select member** list.



10. In the Add role assignment dialog | Review + assign page, click the **Review + assign** button if you see your new Member Role in the Members field.