


# AAD Authentication

Last updated by | Hamza Aqel | Mar 8, 2023 at 2:39 AM PST

This is the public documentation for AAD configuration <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-sign-in-aad-authentication> 

When using AD groups, the current implementation requires that the user chooses to sign in with one of the two groups. When connecting, they would use the Azure AD group name they want to utilize as the username for the database, and that would determine which set of permissions they have.

For example:

User ABC in Azure AD is member of groups DBReadOnly and DBWrite.


The Azure AD administrator would run the following statements on the database:

```
CREATE ROLE "DBReadOnly" WITH LOGIN IN ROLE azure_ad_user;
CREATE ROLE "DBWrite" WITH LOGIN IN ROLE azure_ad_user;
```


They would then run the following to GRANT access for these groups:

```
GRANT SELECT ON ALL TABLES IN SCHEMA public TO "DBReadOnly";
GRANT ALL ON ALL TABLES IN SCHEMA public TO "DBWrite";
```

Now they could choose to connect like this with the DBReadOnly group:

- Hostname: [myserver.postgres.database.azure.com](https://myserver.postgres.database.azure.com) 
- Username: DBReadOnly@myserver
- Password: (output of "az account get-access-token --resource-type oss-rdbms" whilst logged in as user ABC)

## Few notes:

- Azure Active Directory User needs to match UPN:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/howto-troubleshoot-upn-changes> 
- Logins are case sensitive, you can list users in PostgreSQL using:

```
SELECT r.rolname as username,r1.rolname as "role"
FROM pg_catalog.pg_roles r JOIN pg_catalog.pg_auth_members m
ON (m.member = r.oid)
JOIN pg_roles r1 ON (m.roleid=r1.oid)
WHERE r.rolcanlogin ORDER BY 1;
```

- If users has spaces in their names, please use escape character before space, for instance:

Username = DB read only@myserver

needs to be:

Username = DB\ read\ only@myserver

- AAD groups must be "mail enabled security" or "security" group type. You can check this, by searching for Azure Active directory in Azure portal, then search for group and you will see group type, similar to

screenshot below:

Home > Microsoft > Groups



## Groups | All groups

Microsoft - Azure Active Directory

All groups

Deleted groups

Diagnose and solve problems

### Settings

General

Expiration

Naming policy

### Activity

Privileged access groups (Preview)

Access reviews

Audit logs

Bulk operation results

### Troubleshooting + Support

New support request

+ New group Download groups Delete Refresh Columns Preview features Got feedback?

oss

Add filters

	Name	Object Id	Group Type	Membership Type
<input type="checkbox"/>	OS OSS	42c2c15c-d42f-4440-98da-89e...	Microsoft 365	Assigned
<input type="checkbox"/>	OS OSS-AKAMS-ADMIN	1dae5f61-0e39-458a-bc0f-84b...	Mail enabled security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN	6f6051d5-5a9a-441d-ba16-b1...	Mail enabled security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	11e335e9-dcc9-4d12-94e6-1d...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	723f9807-97d0-42ce-962e-cdf...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	22201127-959a-4638-bc44-c5...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	85f824e9-360c-4510-8e6d-478...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	37bd0895-8093-4960-9a22-9b...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	1be0a130-9f47-4bf6-88ff-ccc9...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	2a977cfa-8eaa-41e1-a53d-ea0...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	a04af457-4737-4536-bdf9-ffe...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	d92c3bc3-0ce7-4b63-972f-900...	Security	Assigned
<input type="checkbox"/>	OS OSS-AZURE-ADMIN-SC...	...	...	...

If a customer reports that he can't login with an AAD user that is part of AAD group, you can check the below tips:

- Check the error message as per our TSG [PostgreSQL AAD connectivity](#).
- Look at the above notes on this TSG.
- Make sure that the user is part of the AAD Admin group the customer has added as admin
- Is this a new user added to the AAD group, if yes, we have seen cases based on customers' AAD tenant setting that it could take around 24 hours for the credentials to propagate into the system. It will be good to evaluate this.
- It is good to try adding the failed user as an explicit AAD user than the admin and try to connect.
- If the above attempts did not help, we suggest to engage our Product Group through ICM so they can enable extra logging for more details.

\*\*How good have you found this content?\*\*

