

Azure Active Directory (AAD) SQL logins for Azure SQL DB

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:34 AM PDT

Contents


- [Overview](#)
- [Public Documentation on usage of SQL Logins:](#)
- [Contact](#)


Overview

Azure SQL DB currently supports DB scoped/contained AAD users.

AAD logins (Azure AD server principals) are similar to SQL logins in Azure SQL DB. The benefits from AAD LOGINS are the same as what Azure SQL DB SQL LOGINS.

Customers can introduce an Azure AD login in master db, create users from this login, and with the following permissions(db_manager,loginmanager) to these users, which will allow these users to create new logins and create new dbs . This way customers can have logins as close as to having multiple AAD admins with db_manager and loginmanager roles similar to how it works for SQL logins in Azure SQL DB.

- Public [documentation](#)  on dbmanager and loginmanager role can be found here.

This feature enables AAD logins for SQL DB and Azure Synapse Analytics Note that the AAD logins are already supported for Managed Instance- see [documentation](#) 

In Geo-Replication: They can have read-only access to a user DB by disabling the login on the primary database and allowing a user to access only the secondary database.

If customers are using AAD only authentication (see the CSS TSG on AAD only authentication (Pending to Link)), where only Active Directory based authentication is used, and no SQL authentication, the AAD logins will provide a solution for SQL logins replacement if they are used in Azure SQL db.

Public Documentation on usage of SQL Logins:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/logins-create-manage#create-additional-logins-and-users-having-administrative-permissions> 

Contact

- Contact Team: Azure SQL DB AAD / Security.
- Contact Alias: SQLAADFeedback@microsoft.com, ksec@microsoft.com
- IcM Queue: Azure SQL DB: Security-AAD

How good have you found this content?

