# Azure AD Auth Only - Customers Issues and Troubleshooting

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

Contents


- Customer issues and Troubleshooting:


## Customer issues and Troubleshooting:

### I. Customer tries to add Azure AD Only Authentication property, but does not supply one or more of the AAD Administrator Credentials

The correct error message for the missing credential is usually indicated in the ARM call, we need all AAD Administrator credentials to be supplied for the AAD administrator to be created, and we need the AAD administrator to be created to use AAD Only Authentication.

Eg. {"error":{"code":"ExternalAdministratorPrincipalType","message":"Invalid or missing external administrator principal type. Please select from User, Application or Group."}}

### II. Customer tries to not supply SQL Admin credentials but AAD Only is not turned on

{"name":"a1d3b558-8a43-4811-b867-7037b6d587da","status":"Failed","startTime":"2021-04-19T20:20:23.333Z","error":{"code":"InvalidParameterValue","message":"Invalid value given for parameter Login. Specify a valid parameter value."}}

The SQL Administrator credentials are optional only when a TRUE value for AD Only Authentication has been supplied.

### III. Customer tries to reset SQL Administrator Password when AAD Only is turned on

The operation will fail with 'Reason: Azure Active Directory only authentication is enabled. Please contact your system administrator. '

### IV. Customer request fails with 403 Forbidden where error message suggests they don't have enough permissions to perform the action

Anyone who has permissions to create a new server/MI will have the permissions to set ad only during provisioning and set the AAD Administrator using this API.

### V. Customer tries to update the value of AAD Only Authentications or AAD Administrator using Server / Managed Instance API

This operation will not fail, but it will not update the values since these values are only supported in CREATE server/Managed Instance APIs. Please refer to the `Existing Documentation` section for details on how to update AAD Only Authentication and AAD Administrator via the dedicated APIs i.e.

1. Microsoft.Sql/servers/azureADOnlyAuthentications

1. Microsoft.Sql servers/azureADOnlyAuthentications
2. Microsoft.Sql managedInstances/azureADOnlyAuthentications
3. Microsoft.Sql servers/administrators
4. Microsoft.Sql managedInstances/administrators

**VI. Customer tries to set the value of azureADOnlyAuthentications/aad administrator during provisioning and the operation times out.**

1. This usually means an issue with server / MI creation.
2. Based on this timestamp, run this Kusto Query

MonManagementOperations

| where operation_parameters contains "<server or MI name>"

3. Check the operation parameters, and the workflow results. Note the error message.
4. If the operation parameters suggest that AzureADOnlyAuthentication is not null and External Administrator properties are supplied, and this is a create server request, check the exception, or error message.
5. If the error message suggests an issue with external administrators or azure ad only authentications, create an IcM and assign to **Azure SQL DB: Security and Metadata.**

VII. Customer is not able to use SQL Authentication on the server, and it fails with '**Reason: Azure Active Directory only authentication is enabled. Please contact your system administrator.** '

a. This means that AAD Only Property is true for the customer's server or Managed Instance.

b. Check the XTS View and see if the AAD Only is enabled on the Customer's server/MI and suggest the customer on how to disable it.

c. Please refer to the step-by-step document on how to disable this property.

d. If the property is null/false in the XTS view, create an IcM and assign to **Azure SQL DB: Security and Metadata.**

**Policy WIP**

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