

Azure AD Only Auth - Enable-Disable this Property with Provisioning APIs

Last updated by | Soma Jagadeesh | Aug 11, 2022 at 4:40 PM PDT

Contents


- [How to Enable/Disable this Property with Provisioning APIs:](#)
- [REST API Call - Example Scenario](#)
- [Root Cause Classification](#)

How to Enable/Disable this Property with Provisioning APIs:

1. We only support creating a server or Managed Instance with AAD Only Authentication enabled and AAD Administrator Set.
2. If AAD Administrator properties are not supplied, we will not allow setting AAD Only Authentication to be enabled
3. Customer can not use the Server/Managed Instance APIs to UPDATE the AAD Only Property and AAD Administrator.
4. Customer now has the option to create a new server with AAD Only Enabled, AAD Admin set, and not supplying the SQL Administrator credentials.
5. SQL Administrator Password reset is blocked when AAD Only Authentication is enabled.
6. Customer can use the \$expand=administrators/ActiveDirectory tag to view the administrator and AAD Only resource at the server/managed instance level.
7. Note that while creating the properties during provisioning time the customer must supply a 'principalType' value which can be one of 'User', 'Group' or 'Application'.
8. We currently only support ARM, PowerShell and CLI will be added soon.
9. Only for Managed Instance: After provisioning the Customer still has to set Directory Reader permissions in order to use AAD on MI.

REST API Call - Example Scenario

1. Customer enables AAD Only authentication and AAD Administrator in the CREATE server API call and does not supply a SQL Administrator.

PUT <https://management.azure.com/subscriptions/e1775f9f-a286-0000-b6f0-29c42ac74000/resourceGroups/canarytest/providers/Microsoft.Sql/servers/walmart-test-canaryg2?api-version=2020-11-01-preview> 

```
{
  "location": "eastus2euap",
  "properties": {
    "administrators": { "login": "<login_name>", "sid": "<object_id>", "tenantId": "<tenant_id>", "principalType": "Gro
  }
}
```

2. Customer calls the get server API to fetch administrator & ad only details

GET https://management.azure.com/subscriptions/e1775f9f-a286-0000-b6f0-29c42ac74000/resourceGroups/canarytest/providers/Microsoft.Sql/servers/walmart-test-canaryg2?api-version=2020-11-01-preview&expand=administrators/activeDirectory** [expand=administrators/activeDirectory**]

(https://management.azure.com/subscriptions/SubsscriptionIDNeeded/resourceGroups/canarytest/providers/Microsoft.Sql/servers/walmart-test-canaryg2?api-version=2020-11-01-preview&expand=administrators/activeDirectory)


3. Customer enables AAD Only authentication and AAD Administrator in the CREATE Managed Instance API call and does not supply a SQL Administrator.

PUT <https://management.azure.com/subscriptions/e1775f9f-a286-0000-b6f0-29c42ac74000/resourceGroups/mushahidrg/providers/Microsoft.Sql/managedInstances/walmart-test-gen5-canary2?api-version=2020-11-01-preview> []

```
{
  "name": "walmart-test-gen5-canary2", "type": "Microsoft.Sql/managedInstances", "location": "eastus2euap", "sku
  "properties": {
    "administrators": { "login": "<login_name>", "sid": "<object_id>", "tenantId": "<tenant_id>", "principalType": "Gro
    "subnetId": "/subscriptions/SubscriptionIDNeeded/resourceGroups/mushahidrg/providers/Microsoft.Network/virtual
    "licenseType": "LicenseIncluded", "vCores": 8, "storageSizeInGB": 2048, "collation": "SQL_Latin1_General_CP1_C
    "privateEndpointConnections": [], "storageAccountType": "GRS", "zoneRedundant": false
  }
}
```

4. Customer calls the get server API to fetch administrator & ad only details

GET <https://management.azure.com/subscriptions/SubSubscriptionIDNeeded/resourceGroups/mushahidrg/providers/>

[Microsoft.Sql/managedInstances/walmart-test-gen5-canary2?api-version=2020-11-01-preview&\\$expand=administrators/activeDirectory](https://microsoft.sql/managedInstances/walmart-test-gen5-canary2?api-version=2020-11-01-preview&$expand=administrators/activeDirectory) 

Root Cause Classification

TBD

How good have you found this content?



-