Managed Identities

CSCI E-94

Fundamentals of Cloud Computing - Azure

Joseph Ficara

Agenda

- Overview
- Supported Services
- Limitations
- Azure SQL & Managed Identities

Overview

- Managed Identities:
  - Are “Credentials”
    - Managed by Azure Active Directory
  - Don’t require typical credentials management
    - For resources that support them
- Provide identity for applications to use…
  - When connecting to Azure resources

Overview

- Consist of two types
  - System-assigned
  - User-assigned
- Are formerly known as
  - Managed Service Identity (MSI)

Overview

- Reduced administration & management
  - Automatically managed in Azure Active Directory
  - Security groups for consolidated management
  - **System-assigned** identity
    - **Lifespan is** the **service's lifespan**
  - **User-assigned**
    - Facilitate centralized user access
    - **Lifespan is independent** of the **service's lifespan**

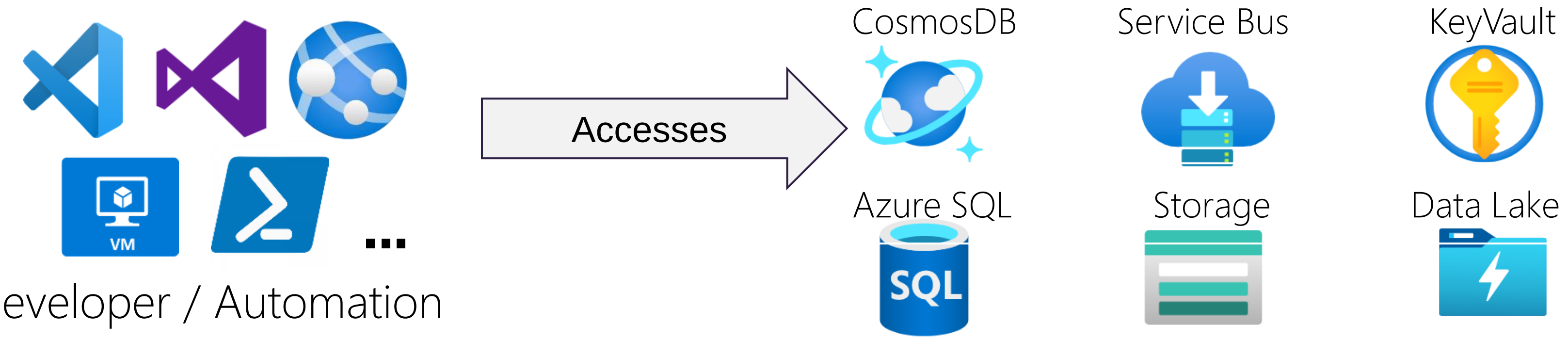
Overview

- Increased security
  - No credentials in
    - Code
    - Configuration files
    - Portal overrides
  - Auto key rotation every 45 days
  - Auto expiration after 90 days
  - CRUD operations in Azure Activity Logs
    - Your mileage may vary depending on service…

Overview

- You can use managed identities when:
  - **The Source**
    - Supports managed identity **assignment**
  - **The Target**
    - Supports **Azure Active Directory authentication**

Source (34+ Supported services) **Target** (9+ Supported services)



CosmosDB
Service Bus
KeyVault
Azure SQL
Storage
Data Lake

Accesses

...

Developer / Automation

Supported Services

- Source Managed identity assignment

Services that can present system or user assigned credentials as their identity

- Azure API Management
- Azure App Configuration
- Azure App Service
- Azure Arc enabled Kubernetes
- Azure Arc-enabled servers
- Azure Automanage
- Azure Automation
- Azure Blueprints
- Azure Cognitive Search
- Azure Cognitive Services
- Azure Container Instances
- Azure Container Registry Tasks
- Azure Data Explorer
- Azure Data Factory V2
- Azure Digital Twins
- Azure Event Grid
- Azure Firewall Policy
- Azure Data Factory V2
- Azure Digital Twins
- Azure Event Grid
- Azure Firewall Policy
- Azure Functions
- Azure IoT Hub
- Azure Import/Export
- Azure Kubernetes Service
- Azure Log Analytics cluster
- Azure Logic Apps
- Azure Machine Learning
- Azure Media Services
- Azure Policy
- Azure Service Fabric
- Azure Spring Cloud
- Azure Stack Edge
- Azure Virtual Machine Scale Sets
- Azure Virtual Machines
- Azure VM Image Builder
- Azure SignalR Service
- Azure Resource Mover
- And more …

And more see docs for updated list…

Supported Services

- **Target** Support Azure Active Directory

  Services that can authenticate and enforce authorization using Microsoft Entra ID System & Managed Identities

  - API Management
  - Azure App Configuration
  - Azure App Services
  - Azure Batch
  - Azure Container Registry
  - Azure Cognitive Services
  - Azure Communication Services
  - Azure Databricks
  - Azure Data Explorer
  - Azure Data Lake Storage Gen1
  - Azure Database for PostgresSQL
  - Azure Digital Twins
  - Azure Event Hubs
  - Azure Iot Hub
  - Azure Key Vault
  - Azure Kubernetes Services (AKS)
  - Azure Machine Learning Services
  - Azure Maps
  - Azure Media services
  - Azure Monitor
  - Azure Resource Manager
  - Azure Service Fabric
  - Azure Service Bus
  - Azure SignalR Service
  - Azure SQL
  - Azure SQL Managed Instance
  - Azure Static Web Apps
  - Azure Storage
  - Azure Virtual Machines

  And more see docs for updated list…

Managed Identity Limitations

- Some limitations to be aware of
  - No support for cloud services
  - Security boundary is associated with
    - Resource it's attached to
  - Not automatically re-created
    - When moving to a new subscription
  - Can't access a resource
    - In a different directory or tenant

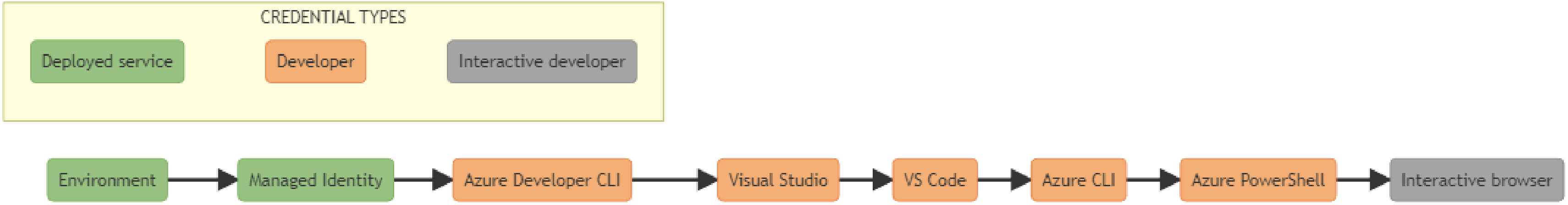
Managed Identity Limitations

- There are rate limits
    - See Azure Instance Metadata Service
        - **20** requests per second, **5** concurrent requests
            - Should be a non-issue in most cases
            - Only happens once during first access per application
- Each managed identity
    - Counts towards object quota limit in Microsoft Entra ID
- Moving user-assigned managed identities
    - to a different resource group is not supported

Managed Identity

DefaultAzureCredential

- Azure Identity client library
  - Provides token authentication support
  - Used across the SDK
  - NuGet Package **Azure.Identity**
  - Facilitates applications running in Azure
  - Attempts to authenticate using this order



Managed Identity

DefaultAzureCredential

- Local development support
  - Visual Studio & Visual Studio Code
    - **DefaultAzureCredential** or **VisualStudioCredential**
  - Azure CLI
  - PowerShell

Managed Identity

DefaultAzureCredential

- Utilizes OAuth with Microsoft Entra ID
  - Support for anything using TokenCredential
  - See: Credential Classes
- Logging can be utilized for diagnostics
  - Via **AzureEventSourceListner**

Managed Identity

DefaultAzureCredential

- When using **User-Assigned Identities**
  - **AZURE_CLIENT_ID** must be configured
    - **Application Id** of the Enterprise application
    - Also referred to as the Client ID
- Note:
  - **AZURE_CLIENT_ID** is not mentioned
    - See: Use managed identity connectivity
    - I submitted a GitHub issue asking for an update

Overview

Azure SQL

Managed Identities

- There are 8 steps required
  - 1. Assign managed identity to the app service
    - 1a. System Assigned

      or
    - 1b. User Assigned
  - 2. Enable Microsoft Entra ID Authentication
    - On the database server
  - 3. Configure an Entra Id user
    - As the Microsoft Entra ID Administrator
  - 4. Connect to the database
    - Using the Microsoft Entra ID Administrator

Azure SQL

Managed Identities

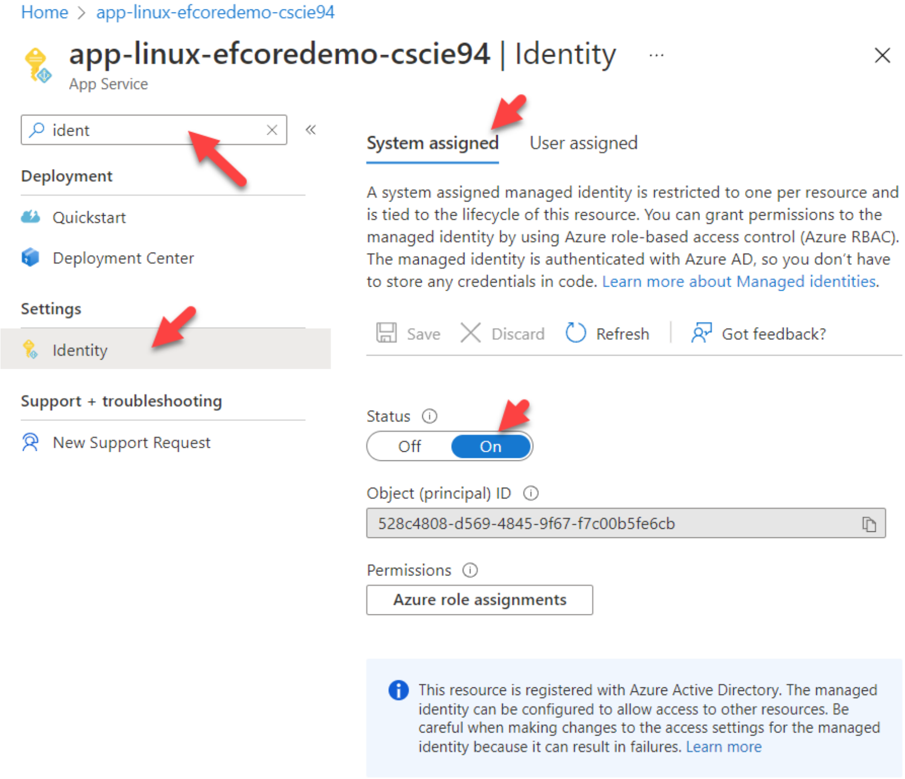
- 5. Add the app services managed identity
  - As a user in the database
- 6. Add these **roles** to the app service's user
  - **db_datareader, db_datawriter, db_ddladmin**
- 7. Modify app service db connection string
  - To use to use managed identity-based credentials
- 8. Add the nuget package
  - **Microsoft.Data.SqlClient**

User Assigned Must set the **AZURE_CLIENT_ID** in portal app settings
Set to the managed identities **ClientId**

Azure SQL

Managed Identities - System Assigned

- 1. Assign managed identity to app service



Home > app-linux-efcoredemo-cscie94

app-linux-efcoredemo-cscie94 | Identity

App Service

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. Learn more about Managed identities.

Status: Off [✓ On]

Object (principal) ID: 528c4808-d569-4845-9f67-f7c00b5fe6cb

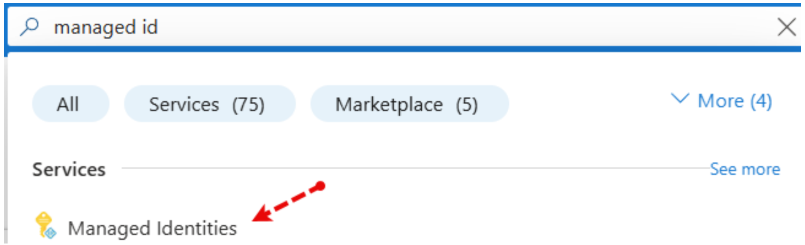
Permissions

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more

Azure SQL

Managed Identities - User Assigned

- Create a Managed Identity

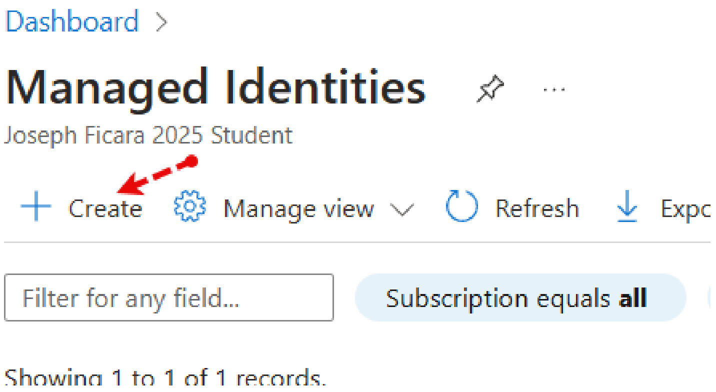


managed id

All | Services (75) | Marketplace (5) | More (4)

Services — See more

Managed Identities



Dashboard >

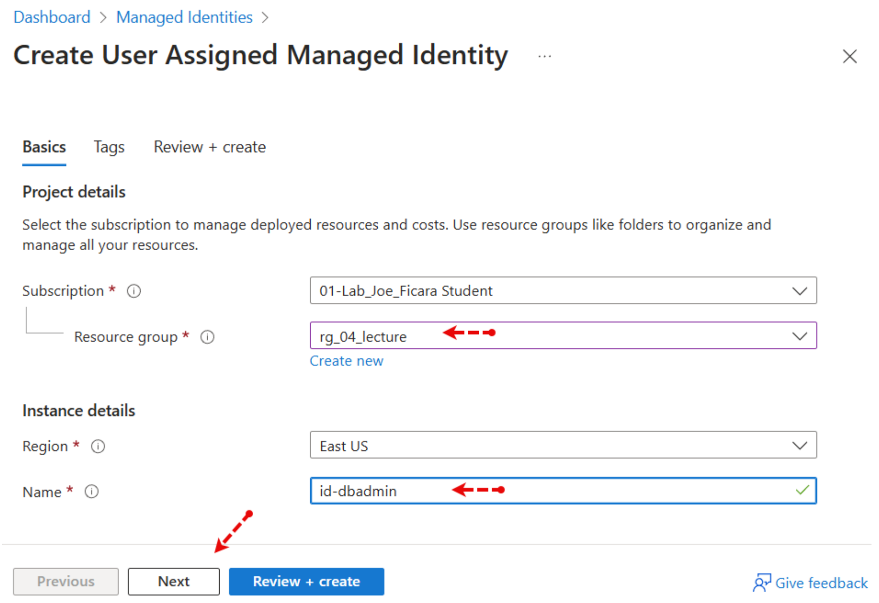
Managed Identities

Joseph Ficara 2025 Student

Filter for any field...

Subscription equals **all**

Showing 1 to 1 of 1 records.



Dashboard > Managed Identities >

Create User Assigned Managed Identity

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : 01-Lab_Joe_Ficara Student

Resource group * : rg_04_lecture

Create new

Instance details

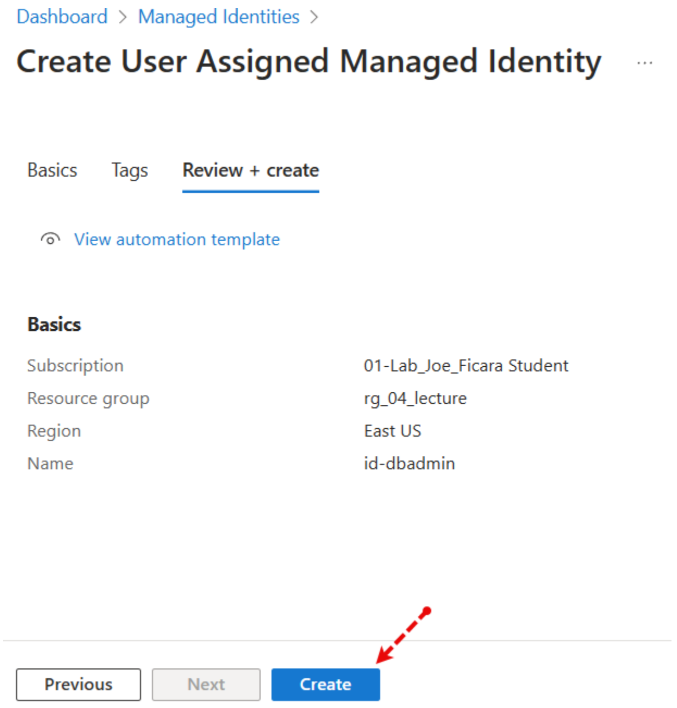
Region * : East US

Name * : id-dbadmin

Azure SQL

Managed Identities - User Assigned

- Create a Managed Identity …



Dashboard > Managed Identities >

Create User Assigned Managed Identity …

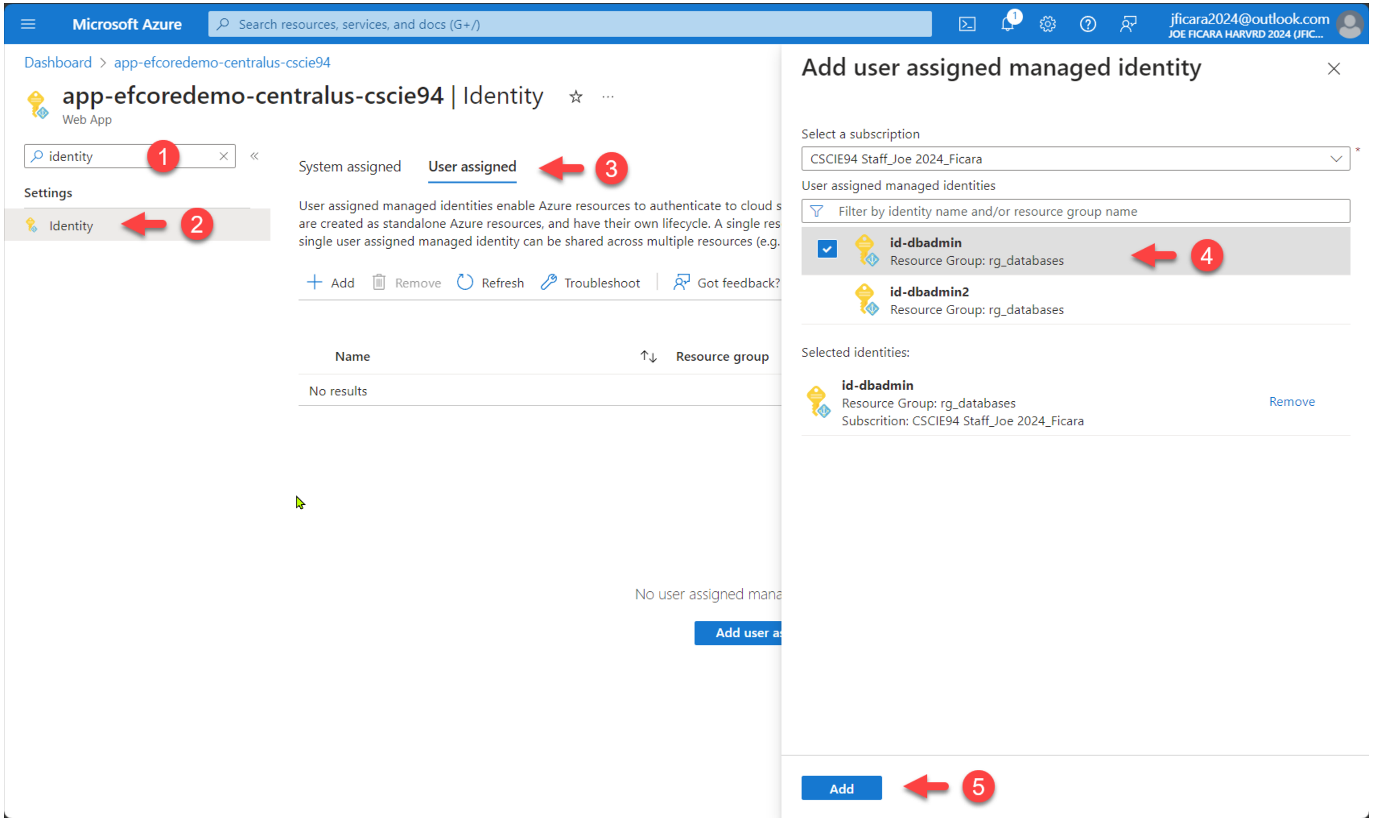
Basics

Subscription	01-Lab_Joe_Ficara Student
Resource group	rg_04_lecture
Region	East US
Name	id-dbadmin

Azure SQL

Managed Identities - User Assigned

- 1. Assign managed identity to app service



Microsoft Azure
Search resources, services, and docs (G+/)
jficara2024@outlook.com
JOE FICARA HARVRD 2024 (JFIC...
Dashboard > app-efcoredemo-centralus-cscie94
app-efcoredemo-centralus-cscie94 | Identity
Web App
identity
1
Settings
Identity
2
System assigned
User assigned
3
Add
Remove
Refresh
Troubleshoot
Got feedback?
Name
Resource group
Add user as
Add user assigned managed identity
4
Remove
Add
5

User assigned managed identities enable Azure resources to authenticate to cloud s are created as standalone Azure resources, and have their own lifecycle. A single res single user assigned managed identity can be shared across multiple resources (e.g.

No results

No user assigned mana

Select a subscription: CSCIE94 Staff_Joe 2024_Ficara

User assigned managed identities

Filter by identity name and/or resource group name

☑ id-dbadmin
Resource Group: rg_databases

id-dbadmin2
Resource Group: rg_databases

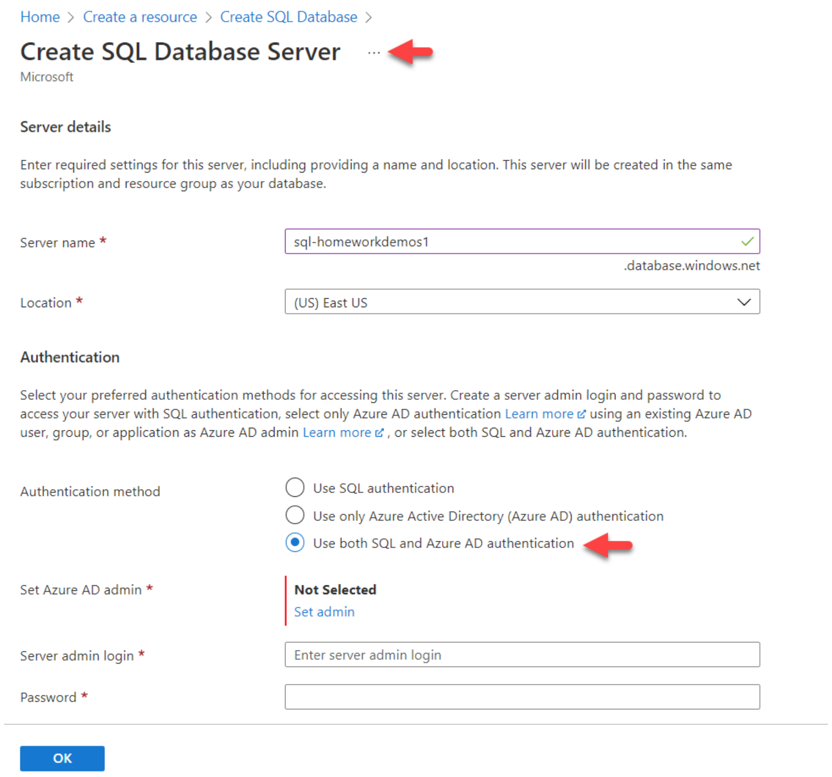
Selected identities:

id-dbadmin
Resource Group: rg_databases
Subscrition: CSCIE94 Staff_Joe 2024_Ficara

Azure SQL

Managed Identities

- 2. Enable Microsoft Entra ID Authentication
  - On the database server



Home > Create a resource > Create SQL Database >

Create SQL Database Server ...

Microsoft

Server details

Enter required settings for this server, including providing a name and location. This server will be created in the same subscription and resource group as your database.

Server name * sql-homeworkdemos1 ✓ .database.windows.net

Location * (US) East US

Authentication

Select your preferred authentication methods for accessing this server. Create a server admin login and password to access your server with SQL authentication, select only Azure AD authentication Learn more using an existing Azure AD user, group, or application as Azure AD admin Learn more , or select both SQL and Azure AD authentication.

Authentication method
○ Use SQL authentication
○ Use only Azure Active Directory (Azure AD) authentication
● Use both SQL and Azure AD authentication

Set Azure AD admin * **Not Selected** Set admin

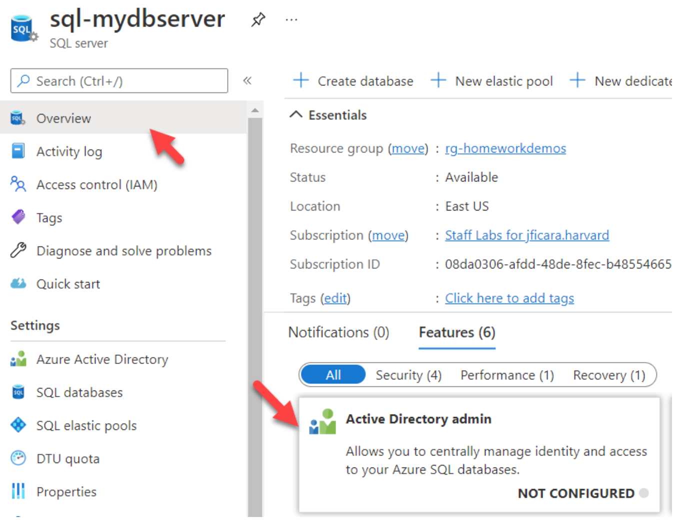
Server admin login * Enter server admin login

Password *

Azure SQL

Managed Identities

- 3a. Configure an Active Directory user
  - As the Microsoft Entra ID Administrator
    - Also enables AD Authentication if not enabled



sql-mydbserver
SQL server

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Quick start

Settings

- Azure Active Directory
- SQL databases
- SQL elastic pools
- DTU quota
- Properties

+ Create database + New elastic pool + New dedicate

Essentials

Resource group (move)	: rg-homeworkdemos
Status	: Available
Location	: East US
Subscription (move)	: Staff Labs for jficara.harvard
Subscription ID	: 08da0306-afdd-48de-8fec-b48554665
Tags (edit)	: Click here to add tags

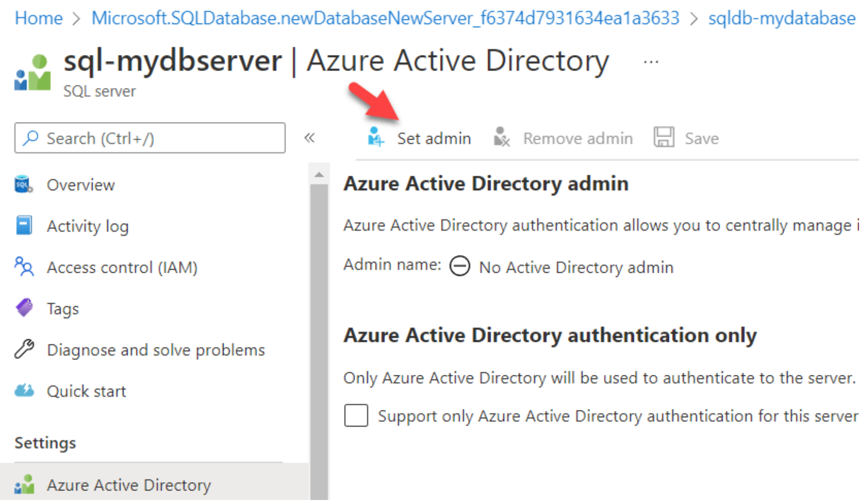
Notifications (0) Features (6)

All Security (4) Performance (1) Recovery (1)

Active Directory admin

Allows you to centrally manage identity and access to your Azure SQL databases.

NOT CONFIGURED



Home > Microsoft.SQLDatabase.newDatabaseNewServer_f6374d7931634ea1a3633 > sqldb-mydatabase

sql-mydbserver | Azure Active Directory ···
SQL server

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Quick start

Settings

- Azure Active Directory

Set admin   Remove admin   Save

Azure Active Directory admin

Azure Active Directory authentication allows you to centrally manage i

Admin name: ⊖ No Active Directory admin

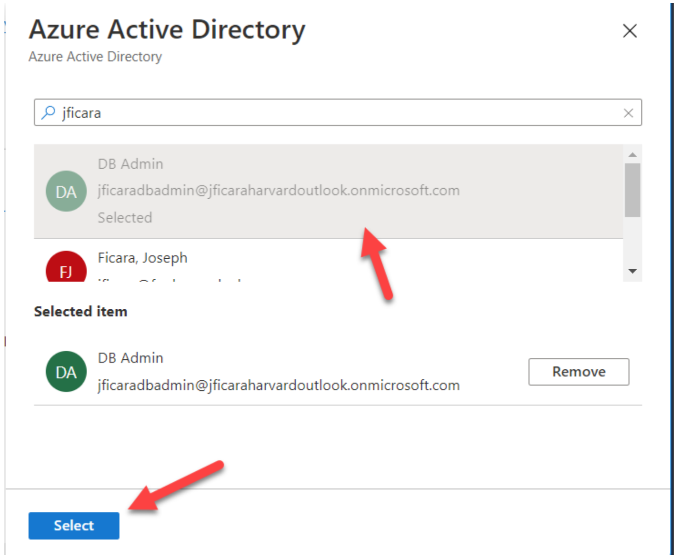
Azure Active Directory authentication only

Only Azure Active Directory will be used to authenticate to the server.

☐ Support only Azure Active Directory authentication for this server

Azure SQL
Managed Identities

- 3b. Configure an Active Directory user
  - As the Microsoft Entra ID Administrator



Azure Active Directory

Azure Active Directory

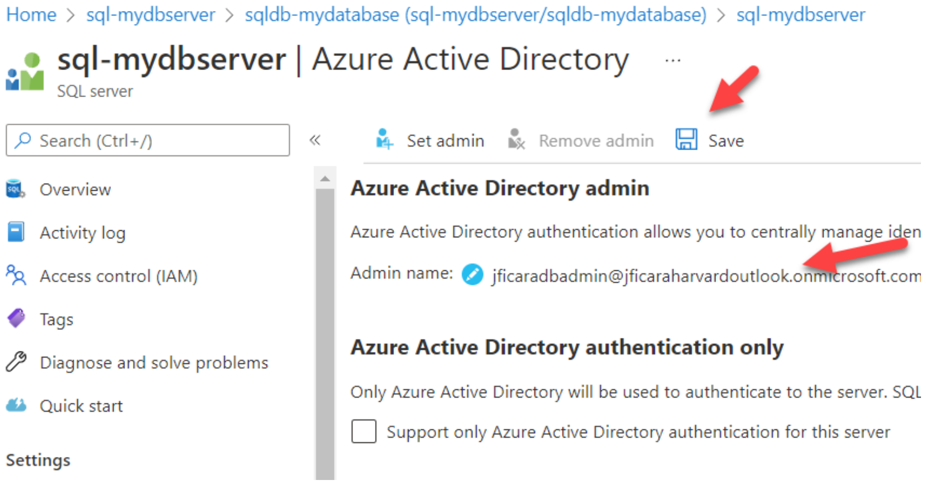
jficara

DB Admin
jficaradbadmin@jficaraharvardoutlook.onmicrosoft.com
Selected

Ficara, Joseph

Selected item

DB Admin
jficaradbadmin@jficaraharvardoutlook.onmicrosoft.com



Home > sql-mydbserver > sqldb-mydatabase (sql-mydbserver/sqldb-mydatabase) > sql-mydbserver

sql-mydbserver | Azure Active Directory

SQL server

Azure Active Directory admin

Azure Active Directory authentication allows you to centrally manage iden

Admin name: jficaradbadmin@jficaraharvardoutlook.onmicrosoft.com

Azure Active Directory authentication only

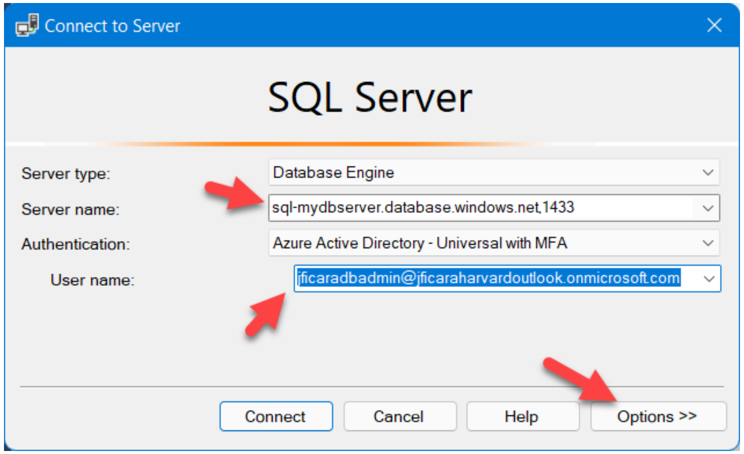
Only Azure Active Directory will be used to authenticate to the server. SQL

□ Support only Azure Active Directory authentication for this server

Azure SQL

Managed Identities

- 4. Connect to the database
  - Using the **Microsoft Entra ID DB Administrator**



Connect to Server

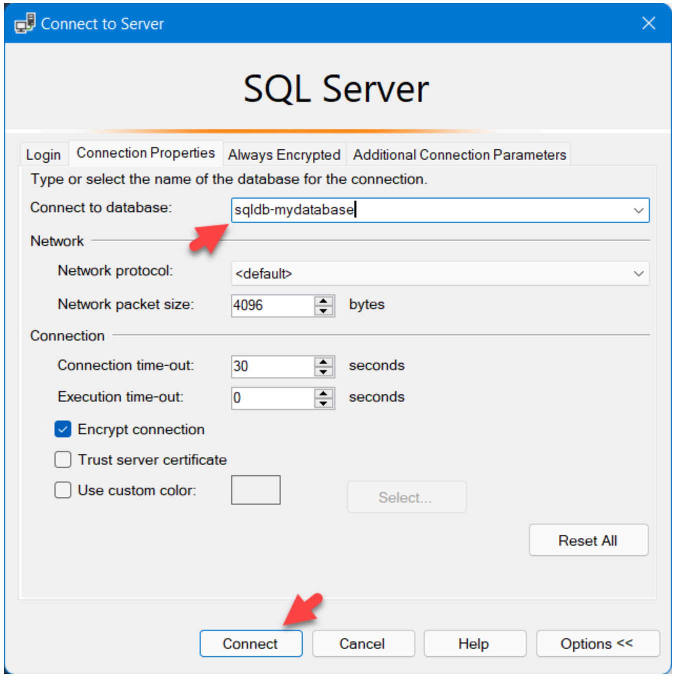
SQL Server

Server type: Database Engine

Server name: sql-mydbserver.database.windows.net,1433

Authentication: Azure Active Directory - Universal with MFA

User name: jficaradbadmin@jficaraharvardoutlook.onmicrosoft.com



Connect to Server

SQL Server

Type or select the name of the database for the connection.

Connect to database: sqldb-mydatabase

Network

Network protocol: <default>

Network packet size: 4096 bytes

Connection

Connection time-out: 30 seconds

Execution time-out: 0 seconds

☑ Encrypt connection

☐ Trust server certificate

☐ Use custom color:

Azure SQL Managed Identities

Steps: 5 & 6 Add user and roles - System Assigned

```
-- 5. Add app services managed identity as a user in the database
CREATE USER [<app service name goes here>] FROM EXTERNAL PROVIDER;

-- 6. Add these roles to the app service's user
--    db_datareader, db_datawriter, db_ddladmin
ALTER ROLE db_datareader ADD MEMBER [<app service name goes here>];
ALTER ROLE db_datawriter ADD MEMBER [<app service name goes here>];
ALTER ROLE db_ddladmin ADD MEMBER [<app service name goes here>];
GO
```

Azure SQL Managed Identities

Steps: 5 & 6 Add user and roles - System Assigned (Example)

```
-- 5. Add app services managed identity as a user in the database
CREATE USER [app-efcoredemo-centralus-cscie94] FROM EXTERNAL PROVIDER;

-- 6. Add these roles to the app service's user
--    db_datareader, db_datawriter, db_ddladmin
ALTER ROLE db_datareader ADD MEMBER [app-efcoredemo-centralus-cscie94];
ALTER ROLE db_datawriter ADD MEMBER [app-efcoredemo-centralus-cscie94];
ALTER ROLE db_ddladmin ADD MEMBER [app-efcoredemo-centralus-cscie94];
GO
```

Azure SQL Managed Identities

Steps: 5 & 6 Add user and roles - User Assigned

```
-- 5. Add app services managed identity as a user in the database
CREATE USER [<managed identity name goes here>] FROM EXTERNAL PROVIDER;

-- 6. Add these roles to the app service's user
--    db_datareader, db_datawriter, db_ddladmin
ALTER ROLE db_datareader ADD MEMBER [< managed identity name goes here >];
ALTER ROLE db_datawriter ADD MEMBER [< managed identity name goes here >];
ALTER ROLE db_ddladmin ADD MEMBER [< managed identity name goes here >];
GO
```

Azure SQL Managed Identities

Steps: 5 & 6 Add user and roles - User Assigned (Example)

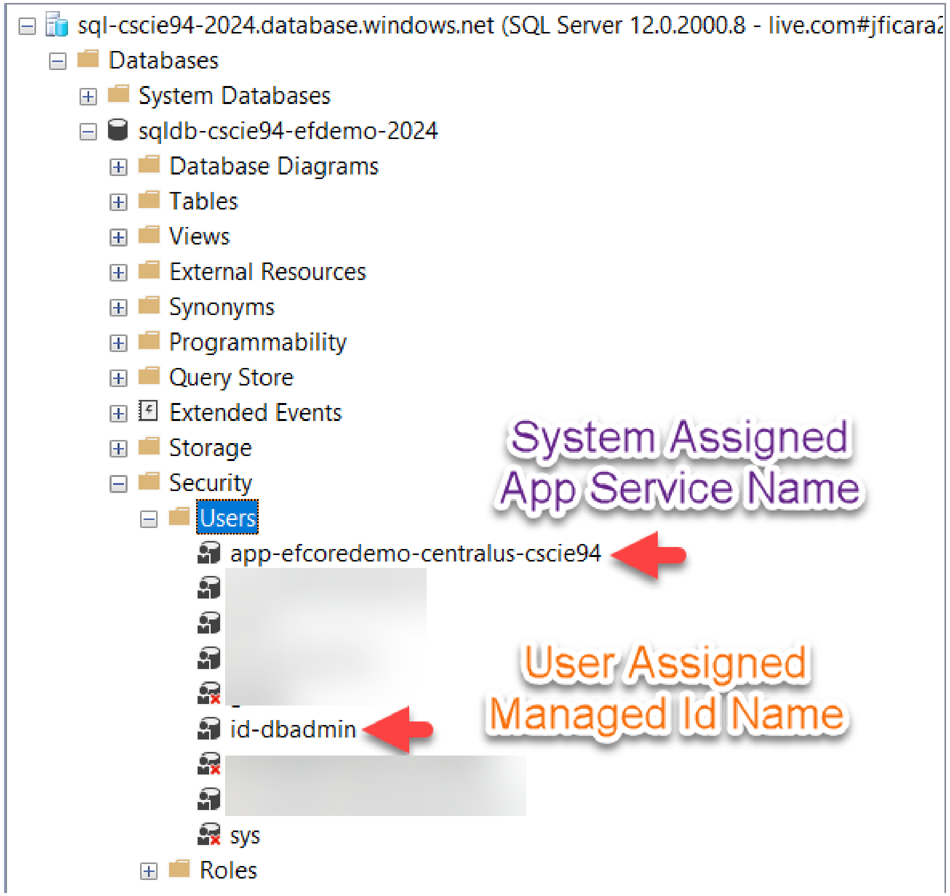
```
-- 5. Add app services managed identity as a user in the database
CREATE USER [id-dbadmin] FROM EXTERNAL PROVIDER;

-- 6. Add these roles to the app service's user
--    db_datareader, db_datawriter, db_ddladmin
ALTER ROLE db_datareader ADD MEMBER [id-dbadmin];
ALTER ROLE db_datawriter ADD MEMBER [id-dbadmin];
ALTER ROLE db_ddladmin ADD MEMBER [id-dbadmin];
GO
```

Azure SQL

Managed Identities

- SSMS: User added to DB



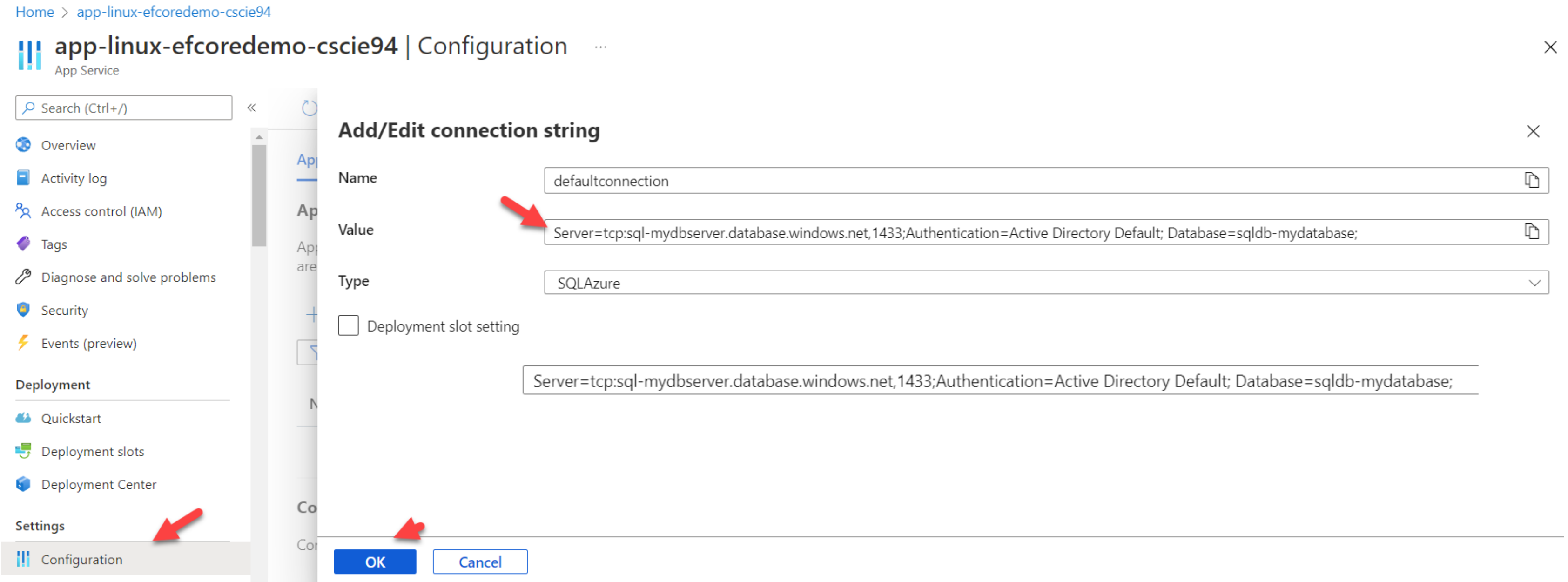
```
⊟ sql-cscie94-2024.database.windows.net (SQL Server 12.0.2000.8 - live.com#jficara
  ⊟ Databases
    ⊞ System Databases
    ⊟ sqldb-cscie94-efdemo-2024
      ⊞ Database Diagrams
      ⊞ Tables
      ⊞ Views
      ⊞ External Resources
      ⊞ Synonyms
      ⊞ Programmability
      ⊞ Query Store
      ⊞ Extended Events
      ⊞ Storage
      ⊟ Security
        ⊟ Users
            app-efcoredemo-centralus-cscie94
            [redacted]
            id-dbadmin
            [redacted]
            sys
        ⊞ Roles
```

System Assigned App Service Name

User Assigned Managed Id Name

Azure SQL
Managed Identities

- 7. Modify app service DB connection string
  - To use to use managed identity-based credentials



Name: defaultconnection

Value: Server=tcp:sql-mydbserver.database.windows.net,1433;Authentication=Active Directory Default; Database=sqldb-mydatabase;

Type: SQLAzure

□ Deployment slot setting

Server=tcp:sql-mydbserver.database.windows.net,1433;Authentication=Active Directory Default; Database=sqldb-mydatabase;

```
Server=tcp:sql-mydbserver.database.windows.net,1433;Authentication=Active Directory Default; Database=sqldb-mydatabase;
```

Azure SQL – Connection String

7. Modify app service DB connection string

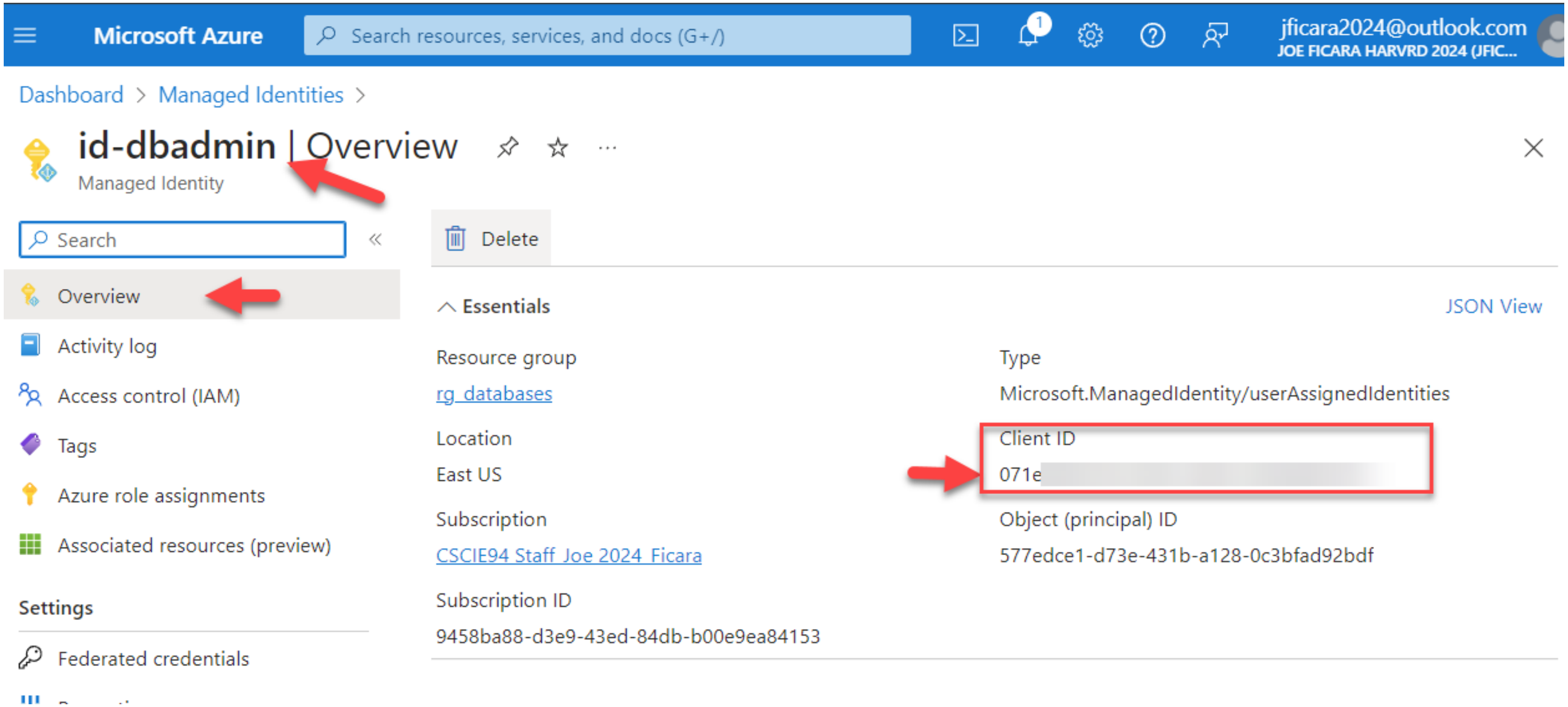
   To use to use managed identity-based credentials

```
Server=tcp:<sqlservername>.database.windows.net,1433;Authentication=Active Directory Default; Database=<databasename>;
```

Azure SQL

Managed Identities – User Assigned

- AZURE_CLIENT_ID
  - Set to the managed identities **ClientId**



Resource group: rg_databases

Location: East US

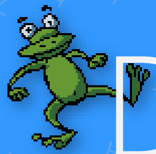
Subscription: CSCIE94 Staff Joe 2024 Ficara

Subscription ID: 9458ba88-d3e9-43ed-84db-b00e9ea84153

Type: Microsoft.ManagedIdentity/userAssignedIdentities

Client ID: 071e[redacted]

Object (principal) ID: 577edce1-d73e-431b-a128-0c3bfad92bdf

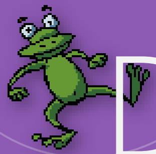


Demo

Azure SQL & Managed Identities

System Assigned Managed Identity

```
EFCoreDemoSolution.sln
app-mi-sys-efcoredemo-cscie94
```



Demo

Azure SQL & Managed Identities

User Assigned Managed Identity

```
EFCoreDemoSolution.sln
app-mi-user-efcoredemo-cscie94
```

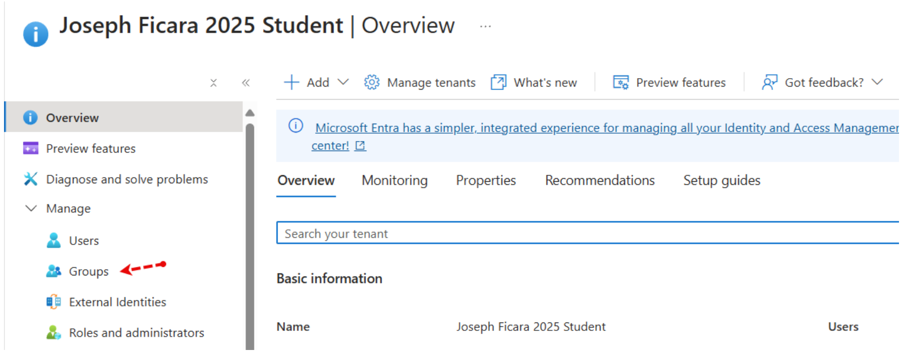
Azure SQL

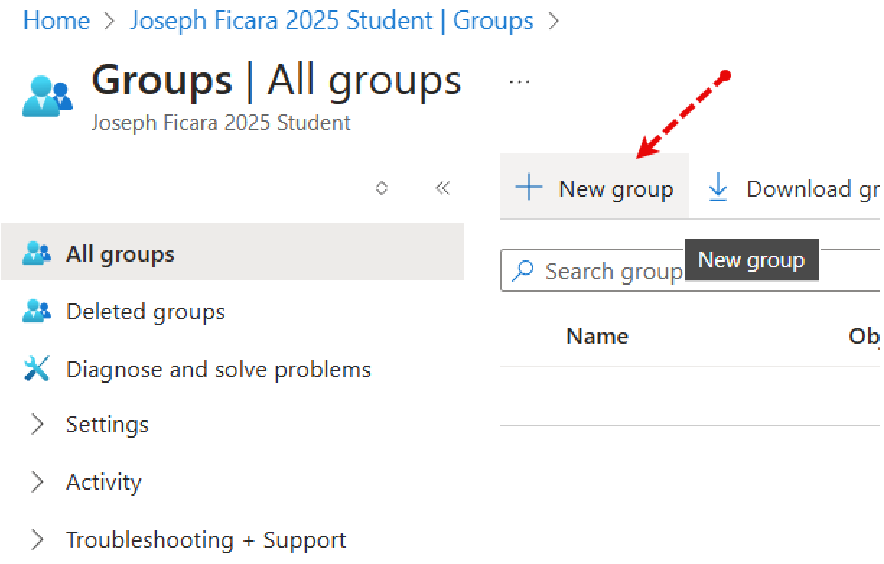
Using a group

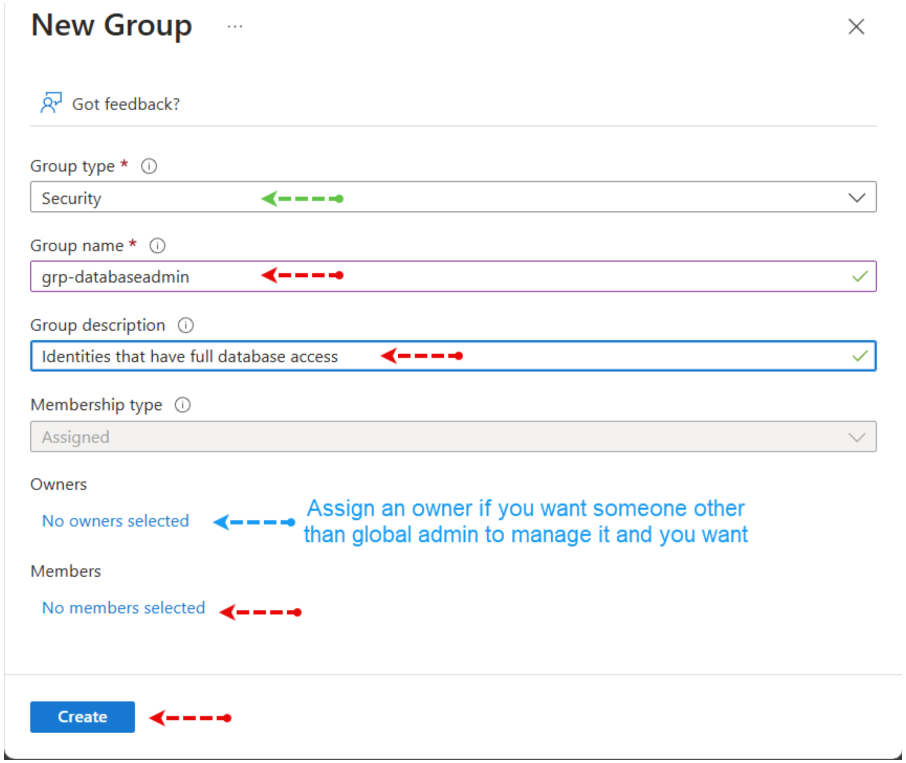
- Easier management
  - Use Groups
- Steps
  - Create the group in Microsoft Entra ID
  - Add the managed identity to the AD Group
  - Add the group to Azure SQL DB
    - The group name is the USER added to SQL

Azure SQL

Creating a group in Microsoft Entra Id




Home > Joseph Ficara 2025 Student | Groups >
Groups | All groups
Joseph Ficara 2025 Student
New group
Download gr
Search group
New group
Name
Ob
All groups
Deleted groups
Diagnose and solve problems
Settings
Activity
Troubleshooting + Support



Group type * Security

Group name * grp-databaseadmin

Group description Identities that have full database access

Membership type Assigned

Owners No owners selected

Members No members selected

Assign an owner if you want someone other than global admin to manage it and you want

Azure SQL

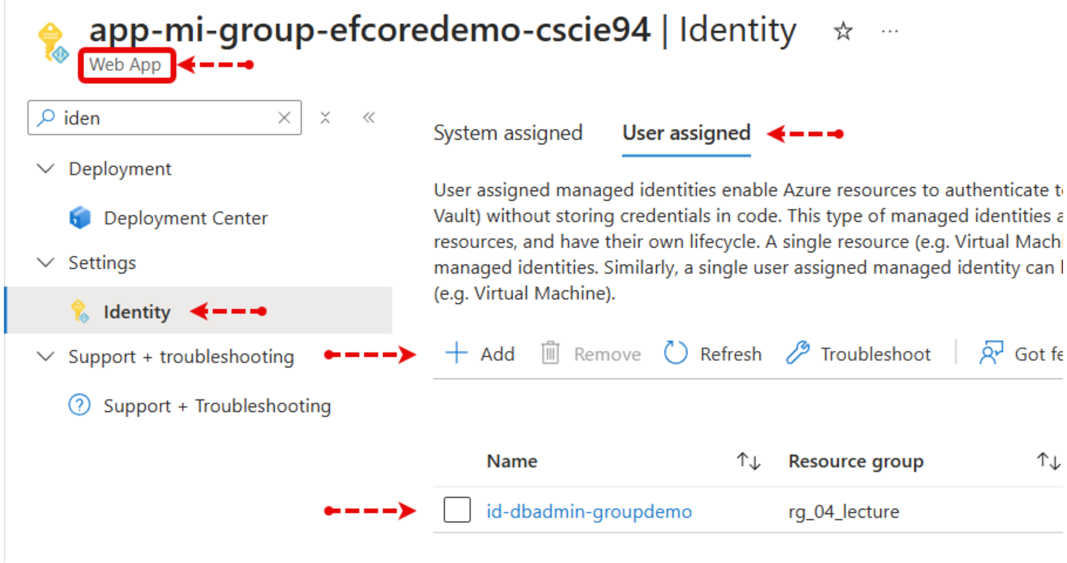
Adding group to Azure SQL DB

```
CREATE USER [grp-databaseadmin] FROM EXTERNAL PROVIDER;
ALTER ROLE db_datareader ADD MEMBER [grp-databaseadmin];
ALTER ROLE db_datawriter ADD MEMBER [grp-databaseadmin];
ALTER ROLE db_ddladmin ADD MEMBER [grp-databaseadmin];
```

Azure SQL

Add the user to the app service

- Don't forget to
  - Add the managed identity
  - That is part of the group to the app service
    - User assigned identity



app-mi-group-efcoredemo-cscie94 | Identity ☆ ···

Web App

User assigned managed identities enable Azure resources to authenticate t
Vault) without storing credentials in code. This type of managed identities a
resources, and have their own lifecycle. A single resource (e.g. Virtual Machi
managed identities. Similarly, a single user assigned managed identity can l
(e.g. Virtual Machine).

	Name ↑↓	Resource group ↑↓
□	id-dbadmin-groupdemo	rg_04_lecture

Demo

Azure SQL & Managed Identities

Group Assignment

```
EFCoreDemoSolution.sln
app-mi-group-efcoredemo-cscie94
```

Azure SQL

Managed Identities

Links & Resources

- Azure SQL & Managed Identities
  - Azure services that can use managed identities to access other services
  - Azure services that support Microsoft Entra ID authentication
  - Tutorial: Connect to SQL Database from App Service without secrets using a managed identity
  - Azure Identity client library for .NET - Azure for .NET Developers | Microsoft Learn