

Create an Azure Active Directory Group

1. Login to the Azure Portal:
 - a. Navigate to <https://portal.azure.com/> and sign in with your Azure credentials.
2. Navigate to **Entra ID**:
 - a. From the left-hand navigation pane, click on "Entra ID"
3. Select Groups:
 - a. Once inside Azure AD, click on "Groups" from the blade's options.
4. Create a New Group:
 - a. Click the "+ New group" button located at the top of the page.
5. Fill in Group Details:
 - a. **Group Type:** By default, this will be set to "**Security**" which is used for assigning access to resources.
 - b. **Group Name:** yourname-db-access
 - c. **Group description:** Optionally, you can provide a description for the group.
 - d. **Membership type:** Determine whether members will be assigned directly or if the group will be a dynamic group where members are added based on rules.
 - i. If you select "Dynamic User" or "Dynamic Device", you will need to set up rules that determine group membership. This is a powerful feature, but requires more configuration.

New Group ...

 Got feedback?

Group type * ⓘ
Security

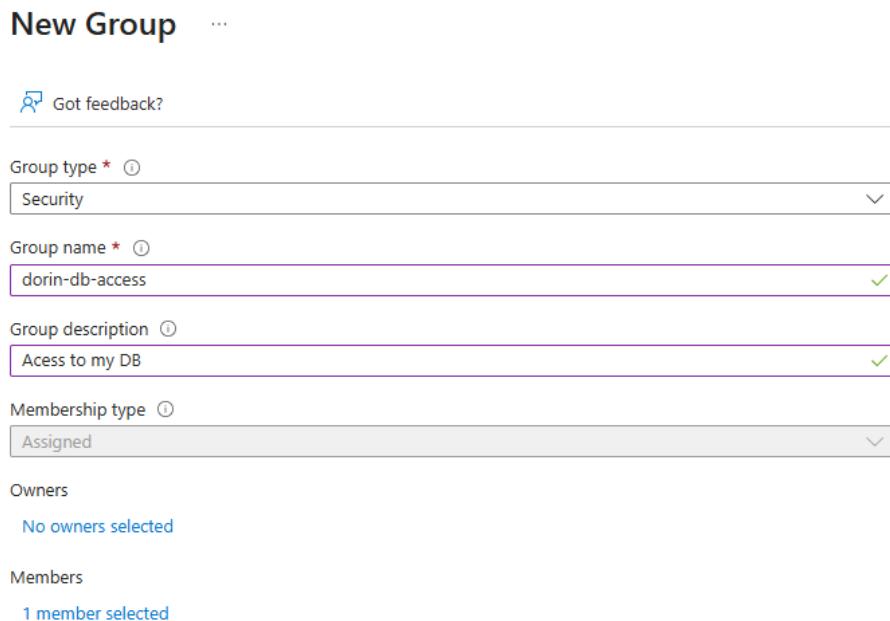
Group name * ⓘ
dorin-db-access

Group description ⓘ
Access to my DB

Membership type ⓘ
Assigned

Owners
No owners selected

Members
1 member selected



6. Add Members (for assigned membership groups):
 - a. Click on the "Members" option and then the "Add members" button.
 - b. Add one of your colleagues to the group
7. Review and Create:

- a. Once all details have been filled in and you've added any necessary members, click the "Create" button at the bottom.

Create an Azure SQL Server

1. Login to the Azure Portal:
 - a. Navigate to <https://portal.azure.com/> and sign in with your Azure account credentials.
2. In the search bar, search for **Sql Server**

The screenshot shows the Azure SQL | SQL logical servers blade. At the top, there's a search bar, a 'Create' button, a 'Manage view' dropdown, and a 'Refresh' button. Below the header, there are navigation links for 'Overview', 'All resources', and 'Azure SQL Database'. Under 'Azure SQL Database', there are three categories: 'SQL databases', 'Hyperscale databases', and 'Elastic pools'. The 'SQL logical servers' category is highlighted with a grey background. At the bottom of the page, there's a link for 'Azure SQL Managed Instance'.

3. Basics Tab:
 - a. **Subscription:** Landing zone A1
 - b. **Resource Group:** yourname-rg
 - c. **Server Name:** Provide a unique name for your SQL Server. This name will be used to form the full DNS name of the server in the format: <server-name>.database.windows.net.
 - d. **Server Admin Login:** Specify the server admin username. Avoid using generic names like 'admin' as they might be disallowed for security reasons.
 - e. **Password:** Enter a strong password for the server admin account and confirm it.
 - f. Set your account as AAD admin account.
 - g. **Location:** West Europe

Create SQL Database Server

Microsoft

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

Subscription * ⓘ

Landing zone A1

Resource group * ⓘ

dorinh-rg

[Create new](#)

Server details

Enter required settings for this server, including providing a name and location.

Server name *

dorin-db

.database.windows.net

Location *

(Europe) West Europe

Authentication

 Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#) ↗

Select your preferred authentication methods for accessing this server. We recommend using only Microsoft Entra authentication [Learn more](#) ↗ using an existing Microsoft Entra user, group, or application as Microsoft Entra admin [Learn more](#) ↗

Authentication method

- Use Microsoft Entra-only authentication
- Use both SQL and Microsoft Entra authentication
- Use SQL authentication

Set Microsoft Entra admin

dorinh@boltinc.com

Admin Object/App ID: 435ddaa3-0700-4b2f-a78c-253ab5388a04

[Set admin](#)

Server admin login *

Enter server admin login

4. Review + Create:

- a. Review your server configuration details.
- b. Click the "Review + create" tab to finalize your choices. Azure will validate your configuration.
- c. Once validation passes, click the "Create" button to start the deployment process.

Create an Azure SQL Database

1. Login to the Azure Portal:

- a. Navigate to <https://portal.azure.com/> and sign in with your Azure credentials.

2. Navigate to SQL Databases:
 - a. Click on "Create a resource" in the top left corner.
 - b. In the "Search the Marketplace" box, type "SQL Database" and select it from the dropdown.
 - c. On the SQL Database page, click the "Create" button.
3. Basic Settings:
 - a. **Subscription:** Select your Azure subscription.
 - b. **Resource Group:** youname-rg
 - c. **Database Name:** youname-database
 - d. **Server:** Select your previously created server
 - e. Want to use SQL elastic pool?: Decide whether you want your database to be part of an elastic pool. If yes, you can select or create an elastic pool here.
 - f. **Compute + storage:** Configure the performance tier, data max size, and other configurations based on your requirements.

Configure ...

 Feedback

Service and compute tier

Select from the available tiers based on the needs of your workload. The vCore model provides a wide range of configuration controls and offers Hyperscale and Serverless to automatically scale your database based on your workload needs. Alternately, the DTU model provides set price/performance packages to choose from for easy configuration. [Learn more](#)

 SQL Database Hyperscale: Low price, high scalability, and best feature set. [Learn more](#)

Service tier

Basic (For less demanding workloads)

[Compare service tiers](#)

DTUs [Compare DTU options](#)

5 (Basic)

Data max size (GB)

								
Cost summary								
<table border="1"> <thead> <tr> <th>Basic (Basic)</th> <th></th> </tr> </thead> <tbody> <tr> <td>Cost per DTU (in USD)</td> <td>0.98</td> </tr> <tr> <td>DTUs selected</td> <td>x 5</td> </tr> <tr> <td>ESTIMATED COST / MONTH</td> <td>4.90 USD</td> </tr> </tbody> </table>	Basic (Basic)		Cost per DTU (in USD)	0.98	DTUs selected	x 5	ESTIMATED COST / MONTH	4.90 USD
Basic (Basic)								
Cost per DTU (in USD)	0.98							
DTUs selected	x 5							
ESTIMATED COST / MONTH	4.90 USD							

Subscription ① Landing zone A1

Resource group ① dorinh-rg

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name * my-db

Server ① dorin-db (West Europe)

Want to use SQL elastic pool? ① Yes No

Workload environment Development Production

ⓘ Default settings provided for Development workloads. Configurations can be modified as needed.

Compute + storage * ①

- Basic
- 2 GB storage
- [Configure database](#)

4. Networking:

- a. Allow Azure services and resources to access this server: You can choose to allow other Azure services to access this server.
- b. **Firewall:** By default, all external access to your new SQL server is blocked by the firewall.
 - i. Add your home IP address to the WAF

Basics **Networking** Security Additional settings Tags Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'dorin-db' and all databases it manages. [Learn more ↗](#)

Firewall rules

The settings displayed below are read-only. They can be modified from the "Firewalls and virtual networks" blade for the selected server after database creation. [Learn more ↗](#)

Allow Azure services and resources to access this server No Yes

Add current client IP address * No Yes

5. Additional Settings:

- a. **Data Source:** Choose if you want to start with an empty database, restore from a backup, or use sample data.
- b. **Collation:** This defines the rules that determine how data is sorted and compared. Choose the appropriate collation if you have specific requirements; otherwise, you can leave the default.
- c. **Advanced Data Security:** Decide if you want to enable advanced data security features for your database.

6. Review + Create:

- Azure will validate your configuration. Once validation passes, click the "Review + create" tab to review your database settings.
- After reviewing, click the "Create" button to start the deployment of your SQL Database.

7. Access and Manage:

- Once deployment is successful, navigate to the "SQL databases" section in the Azure Portal. You should see your newly created database listed there.
- Click on the database to manage, monitor, and perform other operations.

8. Set up Firewalls and Virtual Networks:

- To access your SQL database, you might need to configure firewall rules. This can be done from the "**Firewalls and virtual networks**" option in the database settings. Here you can add your client IP to allow connections.

The screenshot shows the Azure SQL | SQL logical servers blade. On the left, the navigation menu includes 'Overview', 'IL resources', 'Azure SQL Database', 'SQL databases', 'Hyperscale databases', 'Elastic pools', 'SQL logical servers' (which is selected), 'Azure SQL Managed Instance', 'SQL Server', 'Related services', and 'Help'. In the center, the 'dorin-db | Networking' blade is displayed. It has tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Quick start', 'Diagnose and solve problems', 'Resource visualizer', 'Settings', 'Microsoft Entra ID', 'SQL databases', 'SQL elastic pools', 'Properties', 'Locks', 'Data management', 'Security', 'Networking', 'Microsoft Defender for Cloud', 'Transparent data encryption', 'Identity', 'Auditing', and 'Intelligent performance'. The 'Networking' tab is selected. Under 'Public network access', it says 'Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource.' There are two options: 'Disable' (radio button) and 'Selected networks' (radio button, which is selected). Below that, it says 'Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed.' Under 'Virtual networks', it says 'Allow virtual networks to connect to your resource using service endpoints.' Under 'Firewall rules', it says 'Allow certain public internet IP addresses to access your resource.' A rule is listed: 'Add your client IPv4 address (188.27.132.73)' with 'Start IPv4 address' set to '188.27.132.73' and 'End IPv4 address' set to '188.27.132.73'. At the bottom, there are buttons for 'Add a virtual network rule', 'Rule', 'Virtual network', 'Subnet', 'Address range', 'Endpoint status', 'Resource group', 'Subscription', and 'State'.

Connect Azure Data Studio to an Azure SQL Database with AAD

1. Open Azure Data Studio/SQL server

- Launch Azure Data Studio on your computer.

2. Create a New Connection:

- Click on the New Connection icon (or you can find this option in the File menu).

3. Fill in Connection Details:

- Server: Enter the full name of your Azure SQL server, which typically looks like `yourservername.database.windows.net`.
- Authentication type: Choose Azure Active Directory from the dropdown. You'll see several AAD authentication methods, such as:
 - Azure Active Directory - Universal with MFA
 - Azure Active Directory - Password

- iii. Azure Active Directory - Integrated
 - c. Choose the one that best matches your requirements.
 - d. **Username:** Enter your AAD account email (for AAD Password and AAD Universal with MFA methods).
 - e. **Password:** Enter your AAD account password if you're using the AAD Password method.
4. Select Database:
- a. From the Database dropdown, select the specific Azure SQL database you want to connect to. You can also leave it as <Default> to connect to the server without selecting a specific database initially.
5. Advanced Properties (Optional):
- a. You can click on the Advanced button to configure other connection properties if necessary.
6. Initiate the Connection:
- a. Click the Connect button.
7. MFA Users:
- a. If you've chosen the Azure Active Directory - Universal with MFA option, you might be prompted to authenticate using multi-factor authentication. Follow the prompts to complete the authentication process.

Create the table

1. Run the following query

```
CREATE TABLE Employees (
    EmployeeID INT PRIMARY KEY IDENTITY(1,1),
    FirstName NVARCHAR(50),
    LastName NVARCHAR(50),
    Position NVARCHAR(50)
);
```

2. Populate the table with dummy data:

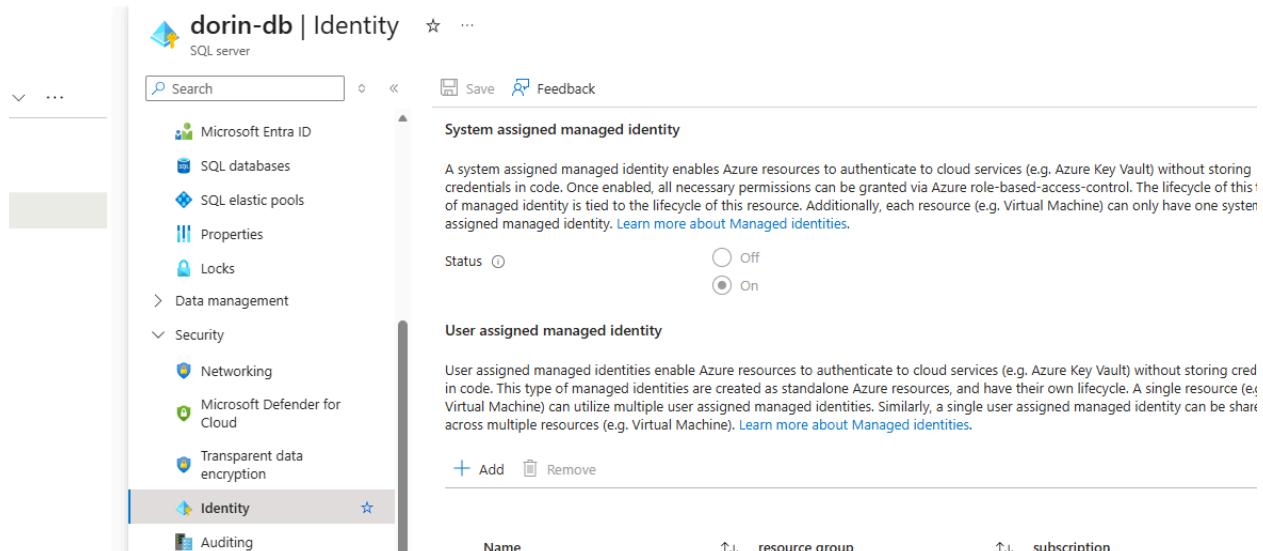
```
INSERT INTO Employees (FirstName, LastName, Position) VALUES
('John', 'Doe', 'Manager'),
('Jane', 'Smith', 'Assistant'),
('Alice', 'Johnson', 'Engineer'),
('Bob', 'Williams', 'Developer'),
('Charlie', 'Brown', 'Designer');
```

3. View the inserted data

```
SELECT * FROM Employees;
```

Create a User in Azure SQL Database for a Service Principal

1. Make sure you have a managed Identity set to your database



The screenshot shows the Azure portal interface for managing identities. On the left, there's a sidebar with options like Microsoft Entra ID, SQL databases, SQL elastic pools, Properties, Locks, Data management, Security, Networking, Microsoft Defender for Cloud, Transparent data encryption, Identity (which is selected), and Auditing. The main content area is titled 'dorin-db | Identity'. It has sections for 'System assigned managed identity' and 'User assigned managed identity'. Under 'System assigned managed identity', there's a note about enabling managed identities for cloud services without storing credentials in code. A status switch is shown, currently set to 'Off'. Below that, under 'User assigned managed identity', there's a note about creating standalone Azure resources with their own lifecycle. A 'Add' button is available to create new user assigned identities.

2. Open Azure Data Studio.

3. Connect to your Azure SQL Database server using your admin account.

4. Execute the following T-SQL commands in Azure Data Studio:

```
-- Use your target database
USE YourDatabaseName;
GO

-- Create a user for the service principal
CREATE USER [your-service-principal-name] FROM EXTERNAL PROVIDER;
GO
```

5. Assign Permissions to the Service Principal (yourname-db-access):

```
-- Grant the service principal read access
EXEC sp_addrolemember 'db_datareader', 'your-service-principal-name';
GO
```