



Azure SQL – Data Masking

What is Data Masking?

Data Masking in Azure SQL Database is a **security feature** that helps protect sensitive data by **obscuring it from unauthorized users** while allowing authorized users to access the original data. Azure SQL Database provides **Dynamic Data Masking (DDM)**, which applies real-time obfuscation without altering the actual data in storage.

For example, a masked credit card number might appear as **XXXX-XXXX-XXXX-1234** instead of the full number.

Benefits of Data Masking

1. Protects Sensitive Data

- Hides personal and confidential data from unauthorized access.

2. No Changes to the Database Structure

- Works at the query level without modifying the actual data.

3. Easy to Implement

- Configured directly in **Azure SQL Database** with simple rules.

4. Reduces Security Risks

- Prevents **accidental data exposure** to non-privileged users.

5. Compliance with Regulations

- Helps meet **GDPR, HIPAA, PCI DSS**, and other data privacy laws.

Use Cases of Data Masking

1. Protecting Personally Identifiable Information (PII)

- Masking names, email addresses, and contact numbers in customer databases.

2. Securing Financial Data

- Hiding credit card numbers, bank account details, and salaries from unauthorized users.

3. Healthcare Data Protection

- Masking patient records, medical history, and insurance details.

4. Development & Testing Environments

- Allowing developers to work with realistic but **obfuscated** data.

5. Preventing Insider Threats

- Ensuring that employees only see **masked sensitive data** based on their roles.

Conclusion

Azure SQL Data Masking is an **efficient and simple way to protect sensitive data** without modifying its actual storage. It helps maintain **data security, privacy, and regulatory compliance** while allowing controlled access to necessary information.

In this lab, we enable Dynamic Data Masking (DDM) in Azure SQL Database to obscure sensitive data from unauthorized users while keeping it accessible to admins. First, log in to SQL Server Management Studio (SSMS) and identify the target column (e.g., email addresses). Then, configure data masking via the Azure Portal by adding a masking rule to the column. Next, create a new user with restricted access and log in as them. The masked data is visible for this user but not for admins.

End Goal: Implement data masking to enhance security, prevent unauthorized data access, and comply with data privacy regulations.

😊 To begin with the Lab

1. In this lab, we will see the data masking feature in Azure SQL Database.
2. The prerequisite for this lab is that you should have the Azure SQL Database running in your Azure portal with sample data loaded on it.
3. So, log in to your SQL Server using SQL Server Management Studio. Here you will see a table with the name Customer.
4. Inside this table you will see a column for email addresses and let's say we want to mask the information for the email address.

The screenshot shows the SSMS interface with the Object Explorer on the left and a query window on the right. The query window displays a result set from a SELECT statement. A red box highlights the 'EmailAddress' column in the results grid, which contains various email addresses for customers. The results grid has columns for SalesPerson, EmailAddress, Phone, and PasswordHash.

SalesPerson	EmailAddress	Phone	PasswordHash
adventure-works\pamel0	orlando0@adventure-works.com	245-555-0173	LRIiwzpz4w7R7VmEg)(X+(A7cXaePEPop+KwQh2JL7w=
adventure-works\david0	keith0@adventure-works.com	170-555-0127	YPdRdvqeAh6wyxEfdshBDNxkCXn+CrgbvJtiknw=
adventure-works\jillian0	donna0@adventure-works.com	279-555-0130	LNaK27abGQo48gGu3EBVUHYSt6V0s7dCRV7uJk=
adventure-works\lillian0	jane0@adventure-works.com	710-555-0173	EzTpSNbUW1U+L5cWfR7MF6nBZia8WpmGaOPjLOJa#
adventure-works\lu0	lucy0@adventure-works.com	828-555-0186	KJqV15wX3PGBTSS5G5ddp6LFFvd3CgrnZM/P0+R4#
adventure-works\linda3	rosmarie0@adventure-works.com	244-555-0112	OKTooczCdizymHHOyJKQICfCILSooS2dQ2Y34VM=
adventure-works\shu0	dominic0@adventure-works.com	192-555-0173	ZooPfZGQm+Xpzz7RKwDHS11YFNbwPVRVT5NnSg=
adventure-works\jose1	kathleen0@adventure-works.com	150-555-0127	Qa3aMCNBVLGrc0b99kbQa/gvWDFhcsK9GZ5UxTM=
adventure-works\jose1	katherine0@adventure-works.com	926-555-0159	uRloVzDGNJIX91+ehTRK+I4UKRgVhAp,jUMC2d4=

5. For that first we will go to our SQL Database on the Portal. Here we have a feature called dynamic data masking. We can choose to add a mask.

The screenshot shows the Azure portal interface for a SQL database named 'demodb'. The top navigation bar includes the database name, a star icon, and a 'SQL database' label. Below the navigation bar is a search bar, save, discard, and 'Add mask' buttons. A red box highlights the 'Add mask' button. On the left, a sidebar lists several features: Auditing, Ledger, Data Discovery & Classification, Dynamic Data Masking (which is highlighted with a red box), Microsoft Defender for Cloud, Identity, and Data Encryption. The main content area is titled 'Masking rules' and contains tabs for 'Schema' and 'Table'. It displays a message: 'You haven't created any masking rules.' Below this, it shows 'SQL users excluded from masking' with a note '(administrators are always excluded)' and a status indicator '(admini... ✓)'. A red box highlights the status indicator.

6. In the add masking rule you can choose the Customer table and then choose the Email column. After that, you have different options to choose the masking field format. Click on Add.

Add masking rule ...

 Add  Delete

Mask name

SalesLT_Customer_EmailAddress

Select what to mask

Schema *

SalesLT

Table *

Customer

Column *

EmailAddress (nvarchar)

Select how to mask

Masking field format

Email (aXXX@XXXX.com)

7. Once it is added click on the save button as well.

 Save  Discard  Add mask

 Feedback

[Learn more - Getting Started Guide](#) 

Masking rules

Schema	Table	Column	Mask Function
SalesLT	Customer	EmailAddress	Email (aXXX@XXXX.com)

8. Now if I come back to SQL Server Management Studio and execute the query again, we will see that the masking does not happen here.
9. It is because we are logged in as the admin user and the masking does not affect your admin level users.

Object Explorer

SQLQuery1.sql - de...odb (sqladmin (89))

```
SELECT TOP (1000) [CustomerID]
    ,[NameStyle]
    ,[Title]
    ,[FirstName]
    ,[MiddleName]
    ,[LastName]
    ,[Suffix]
    ,[CompanyName]
    ,[SalesPerson]
```

	SalesPerson	EmailAddress	Phone	PasswordHash	PasswordS
1	adventure-works\pamel0	orlando0@adventure-works.com	245-555-0173	L/Rlwzpz4w7RwneEgXX+IA7cXaePEPop+KwQh2fJL7w=	1KjXYs4=
2	adventure-works\david8	keith0@adventure-works.com	170-555-0127	YfdtrDvqeAh6wyxFsfshBDNXxxCxn+CrqBjJtknw=	fs1ZGhY=
3	adventure-works\lilan0	donna0@adventure-works.com	279-555-0130	LNoK27abGQo48gGu63EBVUjhSTvViob7dCRV7uJk=	YTNRhRw=
4	adventure-works\jill0	jane1@adventure-works.com	710-555-0173	EzTqSNbuW1Ut+L5cIWR7MF6nBZa8WpmGaQPjLOJA=	nm7D5e4=
5	adventure-works\lu0	lucy0@adventure-works.com	828-555-0186	KJqV1Swx3PGTS5GSddp8LFFFcd3CoRzMiP04+=	cNFKU4w=
6	adventure-works\isha3	rosmane0@adventure-works.com	244-555-0112	OKT0seac0lzmH0ryJK0CIC1LSooS2zdQ2Y34VM=	ihWSQM=
7	adventure-works\ish0	domino0@adventure-works.com	192-555-0173	Zcc0PjZGMm-XpzcTRKwDhs511YFhbybwPVRYTSnG=	sPoUBS0=
8	adventure-works\jos1	kathleen0@adventure-works.com	150-555-0127	Qa3aMCxNbLGco699KsQduVgwYDfHeK9GZSUx0TM=	Ls0SV3g=
9	adventure-works\jos1	katherine0@adventure-works.com	926-555-0159	uRloVzDGNUX9i+ehTIRK+IT4UKRgWhApJgUMC2d4=	jpHKbqE=

Query executed successfully.

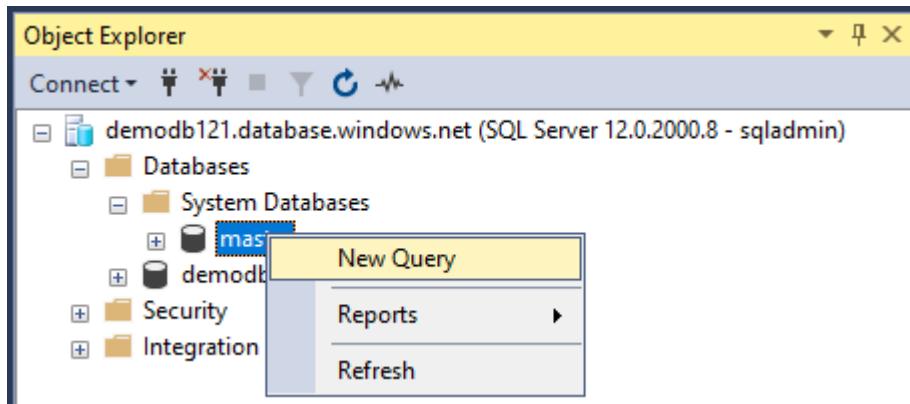
10. For this we are going to create a new user using the below commands and add a role as well to read the data.

```

1 CREATE LOGIN newuser
2      WITH PASSWORD = 'Azure@123'
3 GO
4
5
6 CREATE USER newuser
7      FOR LOGIN newuser
8      WITH DEFAULT_SCHEMA = SalesLT
9
10
11 EXEC sp_addrolemember 'db_datareader', 'newuser';
12
13 DATABASE=demodb

```

11. First you need to expand system databases, then right click on the master database and choose to create a new query.



12. Then a new query page will be opened on the canvas using the same command shown below you have to create a new login for the new user along with the password as shown in the snapshot.
13. Also you can see that we are in the master database as highlighted.

A screenshot of the SSMS interface. The title bar shows 'master' is selected. The Object Explorer on the left shows the database structure. In the center, a query editor window titled 'SQLQuery2.sql - de...ter (sqladmin (80))' contains the following T-SQL code:

```
CREATE LOGIN newuser  
WITH PASSWORD = 'Azure@123'  
GO
```

The status bar at the bottom right indicates 'Query executed successfully.'

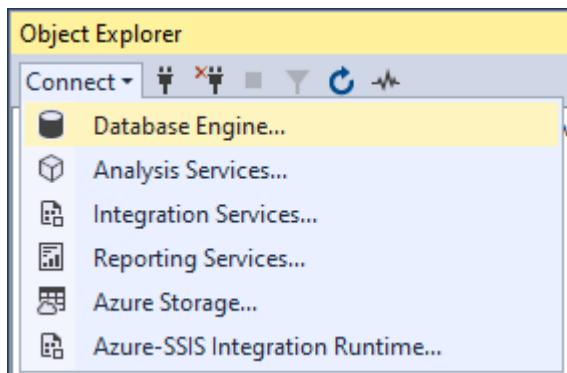
14. Then you need to change your database to demo DB and fire up the remaining commands.

```
CREATE USER newuser  
FOR LOGIN newuser  
WITH DEFAULT_SCHEMA = SalesLT  
  
EXEC sp_addrolemember 'db_datareader', 'newuser';
```

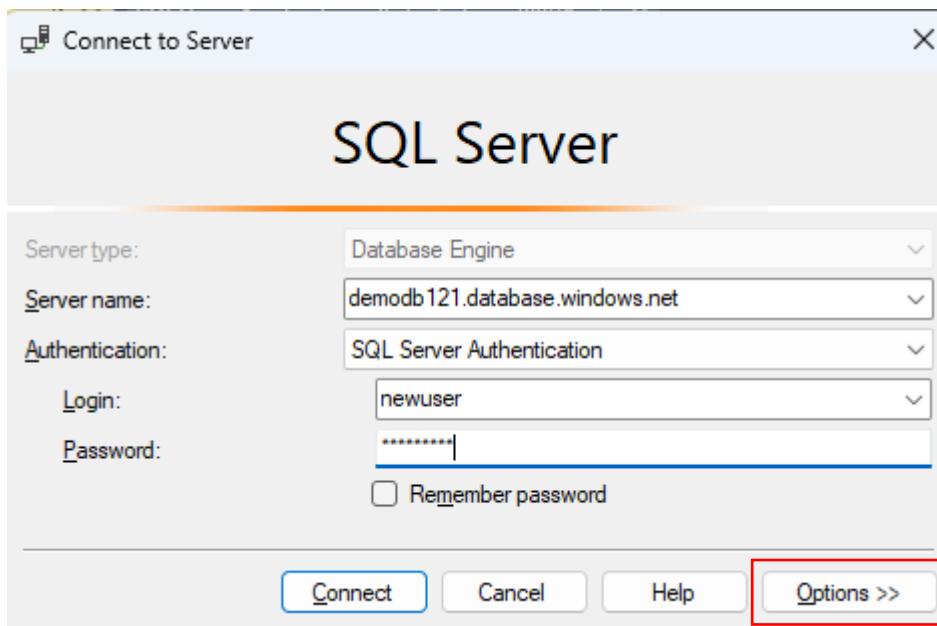
Messages
Commands completed successfully.
Completion time: 2025-03-01T15:58.4766711+05:30

Query executed successfully.

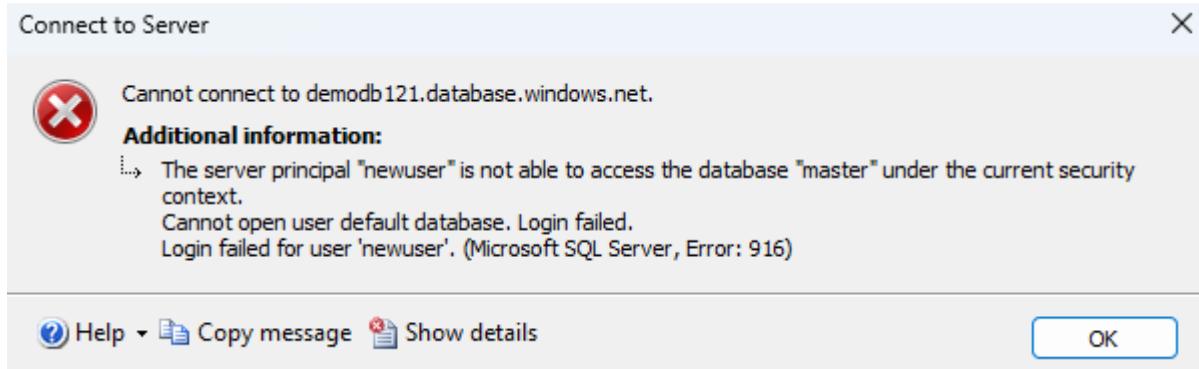
15. Now from the data explorer, click on connect then choose database engine to login as the new user we just created.



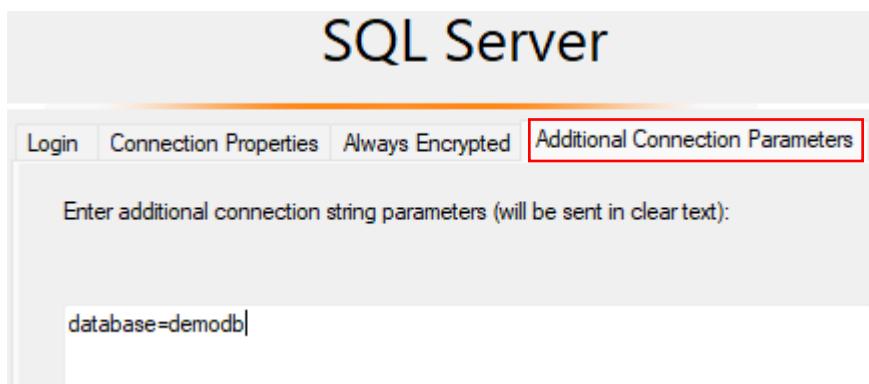
16. Here you just need to give the login name and password, then click on connect.



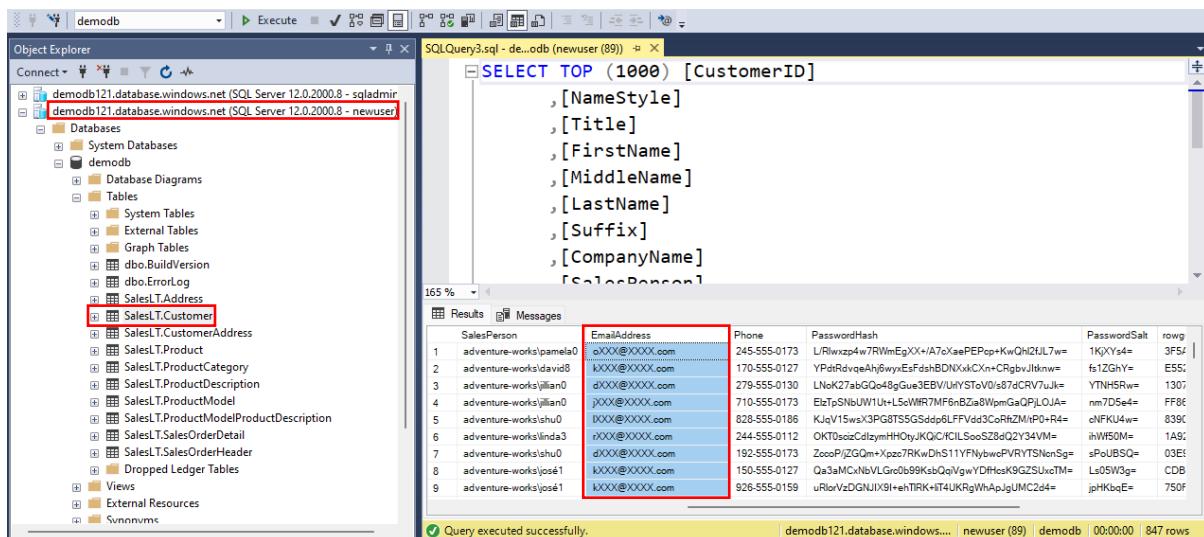
17. So, you will see this error when you click on Connect. To resolve this error, you have to click on the options button as shown above in the snapshot.



18. Then move to Additional connection parameters and here you have to define your database. Click on Connect.



19. Here in the snapshot you can see that we are connected with the new user and when we displayed the data from customer table in the email column we can see the masking.



20. Now if we delete the masking from the portal and save the changes then execute the query again. We can see the email addresses.

demodb

Object Explorer

SQLQuery3.sql - de...odb (newuser (89))

```
SELECT TOP (1000) [CustomerID]
      ,[NameStyle]
      ,[Title]
      ,[FirstName]
      ,[MiddleName]
      ,[LastName]
      ,[Suffix]
      ,[CompanyName]
      ,[SalesPerson]
```

Results Messages

SalesPerson	EmailAddress	Phone	PasswordHash	PasswordSalt
adventure-works\pamel0	orlando0@adventure-works.com	245-555-0173	U/Rlwxp4w7RWImEgXX+ATcXaePEPcp+KwQh2fJL7w=	1KjXYs4=
adventure-works\david8	keith0@adventure-works.com	170-555-0127	YPdtRdvqeAh6wyxEsfshBDNxkCxN+CRgbvJlknw=	f1zGhY+
adventure-works\jillan0	donna0@adventure-works.com	279-555-0130	LNK27abGQo8gGuw3EBV/UHSTv0/s87dCRV7uJk+	YTH5Rw=
adventure-works\jillan0	jane1@adventure-works.com	710-555-0173	EzTpSNdUV1U+LsWFR7MF6nBza8WpmGaOPjLOJA-	nm7D5e4=
adventure-works\lulu0	lucy0@adventure-works.com	828-555-0186	KJv15wsx3PGB7SSGSddp6LFVdd3CcrHzMi/P0+R4=	cNPKU4w=
adventure-works\linda3	rosmane0@adventure-works.com	244-555-0112	OKTosacCdzymHtOyJKQ/CILSooS28dQ2Y34VM=	hWF50M=
adventure-works\linda3	dominic0@adventure-works.com	192-555-0173	ZooP/JZGMw+xpz7RKwDnS11YFnbywPVRYTSMnSg=	sPoUBSQ=
adventure-works\jose1	kathleen0@adventure-works.com	150-555-0127	Qa3MCNbVLGro0s99KsQoQyvwYDffcsK9GZ5Uxu7m=	Ls0SW3g=
adventure-works\jose1	katherine0@adventure-works.com	926-555-0159	uRloVzDGNUIJ91+ehTRK+H4UKRgVhApJgjLMC24+	gHkbqE=

Query executed successfully.

demodb121.database.windows.... newuser (89) | demodb | 00:00:00 | 847 rows