



Azure SQL – Always Encrypted Feature

What is Always Encrypted?

Always Encrypted is a **data security feature** in Azure SQL Database and SQL Server that ensures sensitive data remains encrypted **both at rest and in transit**. Unlike **Transparent Data Encryption (TDE)**, which protects data at rest, **Always Encrypted** ensures that even database administrators (DBAs) or unauthorized users **cannot see or access** the plaintext data.

The encryption and decryption happen **on the client-side** using **encryption keys stored outside the database**, ensuring that **only authorized applications or users can access decrypted data**.

Key Features of Always Encrypted

1. Client-Side Encryption

- Data is **encrypted before being stored** in the database and is decrypted **only by authorized client applications**.

2. Separation of Roles

- Even **DBAs or Azure administrators** cannot access sensitive data.

3. Protects Data in Transit & at Rest

- Unlike TDE, which encrypts only at rest, Always Encrypted ensures **end-to-end encryption**.

4. Column-Level Encryption

- Allows selective encryption of specific columns, such as **credit card numbers or Social Security Numbers (SSNs)**.

5. Integration with Azure Key Vault

- Uses **Azure Key Vault** for secure **key management and rotation**.

Use Cases of Always Encrypted

1. Protecting Sensitive Data

- Encrypting **PII (Personally Identifiable Information)** such as SSNs, medical records, and credit card numbers.

2. Ensuring Regulatory Compliance

- Helps businesses comply with **GDPR, HIPAA, PCI DSS**, and other data security regulations.

3. Securing Financial Transactions

- Used in banking and fintech applications to **encrypt financial transactions and account details**.

4. Healthcare Data Protection

- Ensures **patient data privacy** by encrypting medical records.

5. Preventing Insider Threats

- Ensures that **even database administrators cannot see sensitive data**.

Comparison: Always Encrypted vs. Transparent Data Encryption (TDE)

Feature	Always Encrypted	Transparent Data Encryption (TDE)
Encryption Scope	Column-level	Entire database (storage-level)
Encryption Location	Client-side (before data enters the DB)	Server-side (storage-level)
Protection	Protects data at rest, in transit, and from DBAs	Protects data at rest only
Performance Impact	Higher (due to client-side encryption)	Minimal
Use Case	Protecting highly sensitive data (SSNs, credit cards)	General database encryption (preventing stolen backups from being readable)

Conclusion

Always Encrypted in Azure SQL Database ensures **end-to-end security** by keeping sensitive data encrypted **even from DBAs and Azure administrators**. It is ideal for **financial, healthcare, and regulatory-compliant applications**, offering stronger data protection than **TDE** while ensuring that **only authorized client applications can access decrypted data**.

In this lab, we enable the Always Encrypted feature in Azure SQL Database using Azure Key Vault to secure data at rest and in transit. First, create an Azure Key Vault, configure access policies, and assign cryptographic permissions. Then, in SQL Server Management Studio (SSMS), select a table (e.g., Customer), choose Encrypt Columns, and specify Azure Key Vault for encryption. After encryption completes, the selected column (e.g., email) is encrypted, ensuring protection from unauthorized access.

End Goal: Implement Always Encrypted to enhance data security, confidentiality, and compliance, ensuring only authorized applications can decrypt sensitive data.

To begin with the Lab

- In this lab we will use the always-encrypted feature of Azure SQL Database by making use of Azure Key Vault. We use this feature to encrypt the data at rest or in motion.
- Now to encrypt the data we should have an encrypted key and we have to store that key in the Azure key vault.

3. From the marketplace search for Azure key vault and move to the creation page.
4. Choose your resource group and give a unique key vault name.

Basics Access configuration Networking Tags Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

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

Subscription * MSDN Platforms Subscription ▼

Resource group * NewRG ▼
[Create new](#)

Instance details

Key vault name * demovault121121 ✓

Region * North Europe ▼

Pricing tier * Standard ▼

5. Then on the next option that is Access configuration choose vault access policy and create your key vault.

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

- Azure role-based access control (recommended) ⓘ
- Vault access policy ⓘ

Resource access

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ

6. Then inside your key vault choose access policies then choose the user and click on edit.

The screenshot shows the 'Access policies' section of the Azure Key Vault 'demovault121121' settings. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a prominent 'Access policies' item which is highlighted with a red box. The main area has a search bar, a toolbar with Create, Refresh, Delete, and Edit buttons (the latter is also highlighted with a red box), and a message about access policies. Below that is a table showing one record: a user named 'fabricUser' with email 'fabricUser@behalritesgmail.onmicrosoft.com' and permissions 'Get, List, Update'. There are filters for 'Permissions : All' and 'Type : All'.

Name	Email	Key Permissions
fabricUser	fabricUser@behalritesgmail.onmicrosoft.com	Get, List, Update

7. Then in the permissions you have to assign yourself the Cryptographic operations and click on save.

Cryptographic Operations

[Purge](#)

[Select all](#)

[Decrypt](#)

[Encrypt](#)

[Unwrap Key](#)

[Wrap Key](#)

[Verify](#)

[Sign](#)

Privileged Key Operations

[Select all](#)

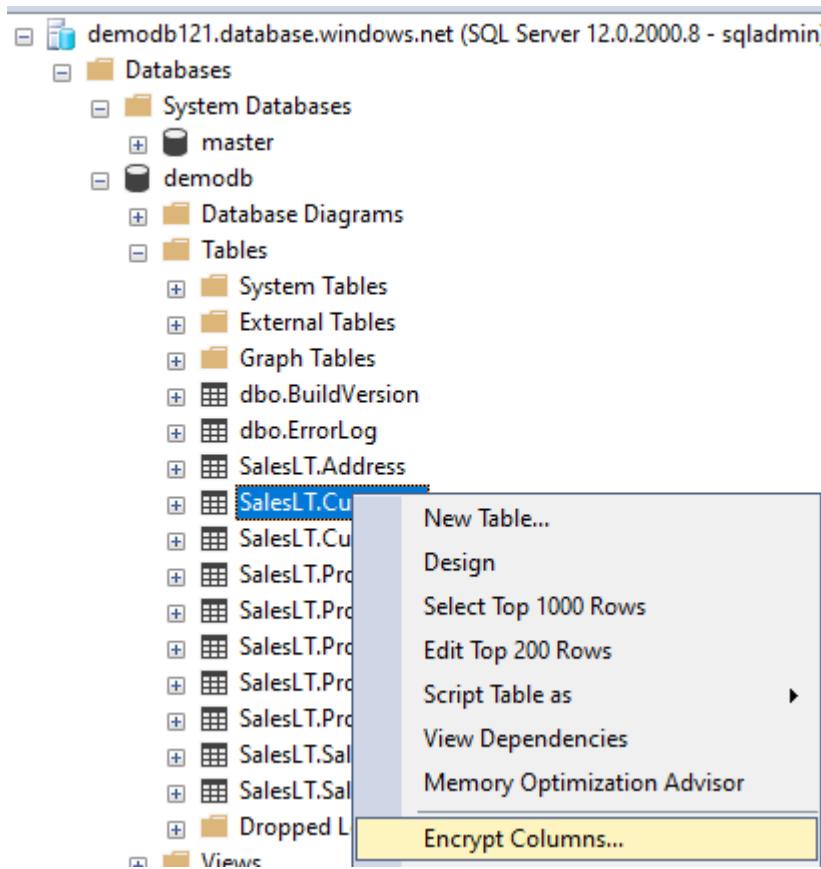
[Purge](#)

[Release](#)

[Previous](#)

[Next](#)

8. Now open your SQL Server Management Studio as the admin user expands your tables then choose the Customer table right click on it and choose Encrypt Columns.

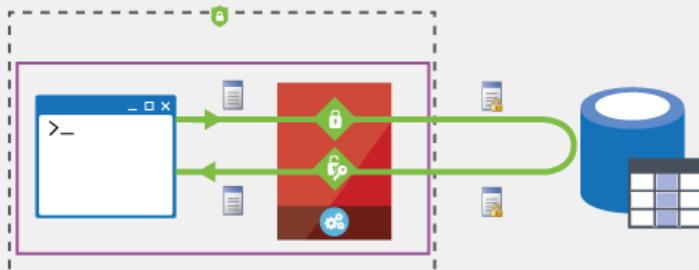


9. You will see that a wizard has been opened. Click on next.

 **Introduction**

Introduction Column Selection Help
Master Key Configuration
In-Place Encryption Settings
Run Settings
Summary
Results

Always Encrypted is a family of industry-leading data protection features that provide a separation between those who own the data and can view it, and those who manage the data but should have no access like high-privileged but unauthorized users. This wizard can be used to encrypt columns for both Always Encrypted and Always Encrypted with secure enclaves.



[Do not show this page again.](#)

< Previous Next > Cancel

10. Now choose which column you want to encrypt and what is the encryption type. Click on next.

Introduction

Column Selection

Master Key Configuration

In-Place Encryption Settings

Run Settings

Summary

Results

Search column name...

Apply one key to all checked columns: CEK_Auto1 (New)

Encryption Type (i) Encryption Key (i)

Name	State	Encryption Type	Encryption Key
SalesLT.Cus...			
Custo...			
NameS...		?	
Title			
FirstNa...			
Middle...			
LastNa...			
Suffix			
Compa...			
SalesPe...			
EmailA...		Deterministic	CEK_Auto1 (New)
Phone			
Passwo...			
Passwo...			
rowguid		?	
Modifi...		?	

Show affected columns only

< Previous Next > Cancel

11. On the next option choose Azure key Vault and click sign in.

Introduction

Column Selection

Master Key Configuration

In-Place Encryption Settings

Run Settings

Summary

Results

Master Key Configuration

To generate a new column encryption key, a column master key must be selected to protect it. The column master key is stored outside of the database.

Select column master key:

Auto generate column master key

Select the key store provider

Windows certificate store (i)

Azure Key Vault (i)

You are not signed in to Microsoft Azure

Sign In...

Select an Azure Key Vault:

12. After signing in you will see your subscription name and the key vault name.

The screenshot shows the 'Master Key Configuration' page in the Azure portal. The left sidebar has a 'Master Key Configuration' tab selected. The main area displays instructions: 'To generate a new column encryption key, a column master key must be selected to protect it. The column master key is stored outside of the database.' It includes a dropdown for 'Select column master key' set to 'Auto generate column master key', and a section for 'Select the key store provider' where 'Azure Key Vault' is selected. Below this, it shows the user is signed in as 'fabricUser@behalriteshgmail.onmicrosoft.com' with a 'Change user' link. A 'Sign Out' button is present. It also shows the 'Select a subscription to use:' dropdown set to 'MSDN Platforms Subscription (d6549a66-c45c-4979-840c-3b356da446b0)' and a 'Select an Azure Key Vault:' dropdown set to 'demovault121121'.

13. Then finish up the things and you will see that a summary page has been opened and here you can see that the encryption is happening. It might take 10-15 minutes to complete.

The screenshot shows the 'Summary' page of the SQL Server Column Encryption Wizard. On the left, a sidebar lists navigation options: Introduction, Column Selection, Master Key Configuration, In-Place Encryption Settings, Run Settings, Summary, and Results. The 'Results' option is selected and highlighted in blue. The main pane displays a summary message: 'Generate new column encryption key CEK_Auto1'. Below this is a progress bar, which is mostly green, indicating task completion. A table titled 'Name' and 'Status' lists three tasks:

Name	Status
Generate new column master key CMK_Auto1 in Azure Key Vault demovault12...	Passed
Generate new column encryption key CEK_Auto1	In Progress...
Performing encryption operations	Not started

14. Once the results are completed you will see every task has been given the status of passed.

The screenshot shows the 'Results' page of the SQL Server Column Encryption Wizard. The sidebar on the left shows the 'Results' option is selected. The main pane displays a summary message: 'Summary:'. Below this is a table titled 'Task' and 'Details' showing the status of three tasks:

Task	Details
Generate new column master key CMK_Auto2 in Azure Key Vault demovault12...	Passed
Generate new column encryption key CEK_Auto1	Passed
Performing encryption operations	Passed

15. Now if we fire up the query once again we can see that our email has been encrypted.

The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer, the database 'demodb' is selected. In the center pane, a query window titled 'SQLQuery4.sql - de...odb (sqladmin (90))' displays the following table structure:

```

[Suffix]
[CompanyName]
[SalesPerson]
[EmailAddress]
[Phone]
[PasswordHash]

```

Below this, the 'Results' tab shows the output of a query:

	SalesPerson	EmailAddress	Phone	PasswordHash
1	adventure-works\pamela0	0x018609BFC5DC67DC9F95A390CD7176229DE0AA332E0F259...	245-555-0173	L/Rlwxp4w7RWmEgXX+A7cXaeI
2	adventure-works\david0	0x0105E199DB17416210FCA32469CC0C7C05A53306D4E42DE...	170-555-0127	Y/PdRvqeAhjwyxyEsFdshBDNx>
3	adventure-works\jillan0	0x01104F951F95B568AF38AA1470D02BEE111D1E2F5E5243...	279-555-0130	LNk2K7abGQ48gGuE3EVU/HY:
4	adventure-works\jillan0	0x01E96176AD88B89C30AC091AE609E8A46C8DAA1C61C093AB...	710-555-0173	EzLzGnbUWU+LsWMr7Mf6gB
5	adventure-works\jillan0	0x0145B7977D92343810F3882330AF02E19AF21E8274337D844...	828-555-0186	KJqV15wsX3PG8TS5GSDp6LFF
6	adventure-works\linda3	0x01E387FF549F9D05E64751897AC85C9BF90A6E6EE41BC...	244-555-0112	OKTUszcCdlzymHHCryJKQCICL!
7	adventure-works\shu0	0x01974067558BE1E83B5B3FD24E47D6859E6C2DC549B2A0...	192-555-0173	Zcc0P/ZGQm+Xpez7RkwDhs11Y
8	adventure-works\jose1	0x01C426B6B698B4093B24D137C69805313D6902080FAA8440...	150-555-0127	Qa3AMCxNbVLGro099KgbQnVg
9	adventure-works\jos1	0x011DFBF169018B385A0000000000000000000000000000000...	926-555-0159	uRloVzDGNJIX9i+e+hTRK+HT4UKf
10	adventure-works\garrett1	0x0143F3FF90F3C7A565011CABE3B1279C4E75A5AA14665...	112-555-0191	jF9jBoFy'eJtEt7x+eJdkd7BzMz
11	adventure-works\jae0	0x01ED03835256703796E60F90DFFED3350FF33E12325C8C1811...	1 (1) 500 555-0132	sK9daCzEKKWaizEGPop0ImaM
12	adventure-works\michael0	0x014F9B89230B217DDA73199418E5E9549D820C66FB24D...	440-555-0132	61zeTkO+eSg0GGswmyWp/6Gz
...

At the bottom of the results grid, it says 'Query executed successfully.'

16. If you go to the key vault and open up the keys you will see a key.

The screenshot shows the Azure Key Vault interface. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, and Objects. Under Objects, the 'Keys' section is selected.

In the main area, there's a search bar and several action buttons: Generate/Import, Refresh, Restore Backup, and Manage deleted keys.

Name	Status
Always-Encrypted-Auto1	✓ Enabled