

Azure SQL database security overview

Azure SQL database storage security overview

Securing your logical server and database configuration



Manage plane security

Securing access to your data



Data Plane security

Encryption in transit



Encryption in transit

Encryption at rest



Encryption at rest

Audit the changes to the data



Auditing






Data plane security basics



- SQL Database supports two types of authentication, SQL Authentication and Azure Active Directory Authentication (Azure AD Authentication).
- **SQL Authentication** - With SQL Authentication, when you create a SQL Database, you also create a login that is the server-level principal account for your SQL Database server.
- **Azure AD authentication** uses identities managed by Azure Active Directory and is supported for managed and integrated domains. To use Azure AD authentication, you must create a second server-level principal account called “Azure AD Admin” to administer Azure AD users and groups. This admin can also perform all operations the regular (SQL) SA can.
- **Server- level roles** - While you can use the server-level principal account to manage server-level security, you also have the option to assign logins to other SQL Database security roles.
- **Database-level roles** - The built-in security roles at the database level are similar to on-premises SQL Server security roles. You can implement database-level security by using fixed database or custom roles for your application

Advanced data security

Advanced data security is a unified package for advanced SQL security capabilities.

	Data discovery & Classification	<ul style="list-style-type: none">• <i>Discover, classify, label & protect the sensitive data in your database</i>• <i>Can be used to provide visibility into your database classification state, and to track the access to sensitive data within the database and beyond its borders..</i>
	Vulnerability assessment	<ul style="list-style-type: none">• <i>Discover, track, and help you remediate potential database vulnerabilities</i>• <i>Provides visibility into your security state, and includes actionable steps to resolve security issues</i>
	Advanced Threat Protection	<ul style="list-style-type: none">• <i>Continuously monitors your database for suspicious activities, and provides immediate security alerts on potential vulnerabilities, SQL injection attacks</i>• <i>Advanced Threat Protection alerts provide details of the suspicious activity and recommend actions</i>

Encryption at rest

- **Transparent Data Encryption (TDE)** has been an on-premises SQL Server option since SQL Server 2008, available exclusively for data at rest. That is, your data files and backups are encrypted, while data tables are not directly encrypted. Specifically, if a user has given permissions to a database with TDE enabled, the user can see all data.
- **Always Encrypted**, which introduces a set of client libraries to allow operations on encrypted data transparently inside of an application. The key is always under control of the client and application, and is never on the server. Neither server nor database administrators can recover data in plain text.

Encryption in transit

- SQL Database connections are encrypted using TLS/SSL for the Tabular Data Stream (TDS) transfer of data. For Azure SQL Database, Microsoft provides a valid certificate for the TLS connection.
- **Row-Level Security** (RLS) restricts access to rows, using a security predicate that is defined as an inline table-valued function (TVF). You create a security policy to enforce this function.
- **Dynamic data masking** - Dynamic Data Masking (DDM) is a feature that allows you to limit access to your sensitive data without making client or application changes, while also enabling visibility of a portion of the data. The underlying data in the database remains intact (data is obfuscated dynamically), and it is applied based on user privilege

- SQL Database auditing is available in all service tiers. By implementing the auditing feature in SQL Database, you can retain your audit trail over time, as well as analyse reports showing database activity of success or failure conditions
- You can configure auditing at the server level. In that case, all databases inherit the same audit settings. As an alternative, you can configure audit policies for each SQL Database individually.