

Overview of SQL Server Security

03/30/2017 2 minutes to read Contributors  [all](#)

In this article

[In This Section](#)

[See Also](#)

A defense-in-depth strategy, with overlapping layers of security, is the best way to counter security threats. SQL Server provides a security architecture that is designed to allow database administrators and developers to create secure database applications and counter threats. Each version of SQL Server has improved on previous versions of SQL Server with the introduction of new features and functionality. However, security does not ship in the box. Each application is unique in its security requirements. Developers need to understand which combination of features and functionality are most appropriate to counter known threats, and to anticipate threats that may arise in the future.

A SQL Server instance contains a hierarchical collection of entities, starting with the server. Each server contains multiple databases, and each database contains a collection of securable objects. Every SQL Server securable has associated *permissions* that can be granted to a *principal*, which is an individual, group or process granted access to SQL Server. The SQL Server security framework manages access to securable entities through *authentication* and *authorization*.

- Authentication is the process of logging on to SQL Server by which a principal requests access by submitting credentials that the server evaluates. Authentication establishes the identity of the user or process being authenticated.
- Authorization is the process of determining which securable resources a principal can access, and which operations are allowed for those resources.

The topics in this section cover SQL Server security fundamentals, providing links to the complete documentation in the relevant version of SQL Server Books Online.

In This Section

[Authentication in SQL Server](#)

Describes logins and authentication in SQL Server and provides links to additional resources.

[Server and Database Roles in SQL Server](#)

Describes fixed server and database roles, custom database roles, and built-in accounts and provides links to additional resources.

[Ownership and User-Schema Separation in SQL Server](#)

Describes object ownership and user-schema separation and provides links to additional resources.

[Authorization and Permissions in SQL Server](#)

Describes granting permissions using the principle of least privilege and provides links to additional resources.

[Data Encryption in SQL Server](#)

Describes data encryption options in SQL Server and provides links to additional resources.

[CLR Integration Security in SQL Server](#)

Provides links to CLR integration security resources.