DENY (Transact-SQL)

05/15/2017 • 5 minutes to read • Contributors

In this article

Syntax
Arguments
Remarks
Permissions
Examples
See Also

THIS TOPIC APPLIES TO: SQL Server (starting with 2008) Azure SQL Database Azure SQL Data Warehouse Parallel Data Warehouse

Denies a permission to a principal. Prevents that principal from inheriting the permission through its group or role memberships. DENY takes precedence over all permissions, except that DENY does not apply to object owners or members of the sysadmin fixed server role. **Security Note** Members of the sysadmin fixed server role and object owners cannot be denied permissions."

Transact-SQL Syntax Conventions

Syntax

Copy

```
-- Syntax for SQL Server and Azure SQL Database

-- Simplified syntax for DENY
DENY   { ALL [ PRIVILEGES ] }
     | <permission>  [ ( column [ ,...n ] ) ] [ ,...n ]
    [ ON [ <class> :: ] securable ]
    TO principal [ ,...n ]
    [ CASCADE] [ AS principal ]
[;]
```

FEEDBACK

```
<permission> ::=
{ see the tables below }

<class> ::=
{ see the tables below }
```

Copy

```
-- Syntax for Azure SQL Data Warehouse and Parallel Data Warehouse

DENY
    <permission> [ ,...n ]
    [ ON [ <class_> :: ] securable ]
    TO principal [ ,...n ]
    [ CASCADE ]
[;]

<permission> ::=
{ see the tables below }

<class> ::=
{
      LOGIN
    | DATABASE
    | OBJECT
    | ROLE
    | SCHEMA
    | USER
}
```

Arguments

ALL
This option does not deny all possible permissions. Denying ALL is equivalent to denying the following permissions.

- If the securable is a database, ALL means BACKUP DATABASE, BACKUP LOG, CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, and CREATE VIEW.
- If the securable is a scalar function, ALL means EXECUTE and REFERENCES.
- If the securable is a table-valued function, ALL means DELETE, INSERT, REFERENCES, SELECT, and UPDATE.
- If the securable is a stored procedure, ALL means EXECUTE.
- If the securable is a table, ALL means DELETE, INSERT, REFERENCES, SELECT, and UPDATE.

- If the securable is a view, ALL means DELETE, INSERT, REFERENCES, SELECT, and UPDATE.

> ⓘ **Note**
>
> The DENY ALL syntax is deprecated. This feature will be removed in a future version of Microsoft SQL Server. Avoid using this feature in new development work, and plan to modify applications that currently use this feature. Deny specific permissions instead.

PRIVILEGES
Included for ISO compliance. Does not change the behavior of ALL.

permission
Is the name of a permission. The valid mappings of permissions to securables are described in the sub-topics listed below.

column
Specifies the name of a column in a table on which permissions are being denied. The parentheses () are required.

class
Specifies the class of the securable on which the permission is being denied. The scope qualifier **::** is required.

securable
Specifies the securable on which the permission is being denied.

TO *principal*
Is the name of a principal. The principals to which permissions on a securable can be denied vary, depending on the securable. See the securable-specific topics listed below for valid combinations.

CASCADE
Indicates that the permission is denied to the specified principal and to all other principals to which the principal granted the permission. Required when the principal has the permission with GRANT OPTION.

AS *principal*
Use the AS principal clause to indicate that the principal recorded as the denier of the permission should be a principal other than the person executing the statement. For example, presume that user Mary is principal_id 12 and user Raul is principal 15. Mary executes `DENY SELECT ON OBJECT::X TO Steven WITH GRANT OPTION AS Raul;` Now the sys.database_permissions table will indicate that the grantor_prinicpal_id of the deny statement was 15 (Raul) even though the statement was actually executed by user 13 (Mary).

The use of AS in this statement does not imply the ability to impersonate another user.

Remarks

The full syntax of the DENY statement is complex. The syntax diagram above was simplified to draw attention to its structure. Complete syntax for denying permissions on specific securables is described in the topics listed below.

DENY will fail if CASCADE is not specified when denying a permission to a principal that was granted that permission with GRANT OPTION specified.

The sp_helprotect system stored procedure reports permissions on a database-level securable.

> ⚠ **Caution**
>
> A table-level DENY does not take precedence over a column-level GRANT. This inconsistency in the permissions hierarchy has been preserved for the sake of backward compatibility. It will be removed in a future release.

> ⚠ **Caution**
>
> Denying CONTROL permission on a database implicitly denies CONNECT permission on the database. A principal that is denied CONTROL permission on a database will not be able to connect to that database.

> ⚠ **Caution**
>
> Denying CONTROL SERVER permission implicitly denies CONNECT SQL permission on the server. A principal that is denied CONTROL SERVER permission on a server will not be able to connect to that server.

Permissions

The caller (or the principal specified with the AS option) must have either CONTROL permission on the securable, or a higher permission that implies CONTROL permission on the securable. If using the AS option, the specified principal must own the securable on which a permission is being denied.

Grantees of CONTROL SERVER permission, such as members of the sysadmin fixed server role, can deny any permission on any securable in the server. Grantees of CONTROL permission on the database, such as members of the db_owner fixed database role, can deny any permission on any securable in the database. Grantees of CONTROL permission on a schema can deny any permission on any object in the schema. If the AS clause is used, the specified principal must own the securable on which permissions are being denied.

Examples

The following table lists the securables and the topics that describe the securable-specific syntax.

Application Role	DENY Database Principal Permissions (Transact-SQL)
Assembly	DENY Assembly Permissions (Transact-SQL)
Asymmetric Key	DENY Asymmetric Key Permissions (Transact-SQL)
Availability Group	DENY Availability Group Permissions (Transact-SQL)
Certificate	DENY Certificate Permissions (Transact-SQL)
Contract	DENY Service Broker Permissions (Transact-SQL)
Database	DENY Database Permissions (Transact-SQL)
Database Scoped Credential	DENY Database Scoped Credential (Transact-SQL)
Endpoint	DENY Endpoint Permissions (Transact-SQL)
Full-Text Catalog	DENY Full-Text Permissions (Transact-SQL)
Full-Text Stoplist	DENY Full-Text Permissions (Transact-SQL)
Function	DENY Object Permissions (Transact-SQL)
Login	DENY Server Principal Permissions (Transact-SQL)
Message Type	DENY Service Broker Permissions (Transact-SQL)
Object	DENY Object Permissions (Transact-SQL)
Queue	DENY Object Permissions (Transact-SQL)
Remote Service Binding	DENY Service Broker Permissions (Transact-SQL)
Role	DENY Database Principal Permissions (Transact-SQL)
Route	DENY Service Broker Permissions (Transact-SQL)
Schema	DENY Schema Permissions (Transact-SQL)
Search Property List	DENY Search Property List Permissions (Transact-SQL)

Server	DENY Server Permissions (Transact-SQL)
Service	DENY Service Broker Permissions (Transact-SQL)
Stored Procedure	DENY Object Permissions (Transact-SQL)
Symmetric Key	DENY Symmetric Key Permissions (Transact-SQL)
Synonym	DENY Object Permissions (Transact-SQL)
System Objects	DENY System Object Permissions (Transact-SQL)
Table	DENY Object Permissions (Transact-SQL)
Type	DENY Type Permissions (Transact-SQL)
User	DENY Database Principal Permissions (Transact-SQL)
View	DENY Object Permissions (Transact-SQL)
XML Schema Collection	DENY XML Schema Collection Permissions (Transact-SQL)

See Also

REVOKE (Transact-SQL)
sp_addlogin (Transact-SQL)
sp_adduser (Transact-SQL)
sp_changedbowner (Transact-SQL)
sp_dropuser (Transact-SQL)
sp_helprotect (Transact-SQL)
sp_helpuser (Transact-SQL)

> **Note**
>
> The feedback system for this content will be changing soon. Old comments will not be carried over. If content within a comment thread is important to you, please save a copy. For more information on the upcoming change, we invite you to read our blog post.

0 Comments

Sign in

2 people listening

+ Follow

Post comment as...

English (United States)

Previous Version Docs • Blog • How to contribute • Privacy & Cookies • Terms of Use • Feedback • Trademarks