What are GRANT, DENY, and REVOKE Permissions

[GRANT](http://msdn.microsoft.com/en-us/library/ms187965.aspx) – this allows the principal to perform an action

[DENY](http://msdn.microsoft.com/en-us/library/ms188338.aspx) – this Denies permission to a login (principal)

[REVOKE](http://msdn.microsoft.com/en-us/library/ms187728.aspx) – These remove the grant or deny permission to the securable

Notes:

A deny will override a grant. This means that if a user is denied permission they cannot inherit a grant from another source

**Viewing the Permissions Script**

SELECT

[UserName] = CASE princ.[type]

WHEN 'S' THEN princ.[name]

WHEN 'U' THEN ulogin.[name] COLLATE Latin1\_General\_CI\_AI

END,

[UserType] = CASE princ.[type]

WHEN 'S' THEN 'SQL User'

WHEN 'U' THEN 'Windows User'

END,

[DatabaseUserName] = princ.[name],

[Role] = null,

[PermissionType] = perm.[permission\_name],

[PermissionState] = perm.[state\_desc],

[ObjectType] = obj.type\_desc,--perm.[class\_desc],

[ObjectName] = OBJECT\_NAME(perm.major\_id),

[ColumnName] = col.[name]

FROM

--database user

sys.database\_principals princ

LEFT JOIN

--Login accounts

sys.login\_token ulogin on princ.[sid] = ulogin.[sid]

LEFT JOIN

--Permissions

sys.database\_permissions perm ON perm.[grantee\_principal\_id] = princ.[principal\_id]

LEFT JOIN

--Table columns

sys.columns col ON col.[object\_id] = perm.major\_id

AND col.[column\_id] = perm.[minor\_id]

LEFT JOIN

sys.objects obj ON perm.[major\_id] = obj.[object\_id]

WHERE

princ.[type] in ('S','U')

UNION

--List all access provisioned to a sql user or windows user/group through a database or application role

SELECT

[UserName] = CASE memberprinc.[type]

WHEN 'S' THEN memberprinc.[name]

WHEN 'U' THEN ulogin.[name] COLLATE Latin1\_General\_CI\_AI

END,

[UserType] = CASE memberprinc.[type]

WHEN 'S' THEN 'SQL User'

WHEN 'U' THEN 'Windows User'

END,

[DatabaseUserName] = memberprinc.[name],

[Role] = roleprinc.[name],

[PermissionType] = perm.[permission\_name],

[PermissionState] = perm.[state\_desc],

[ObjectType] = obj.type\_desc,--perm.[class\_desc],

[ObjectName] = OBJECT\_NAME(perm.major\_id),

[ColumnName] = col.[name]

FROM

--Role/member associations

sys.database\_role\_members members

JOIN

--Roles

sys.database\_principals roleprinc ON roleprinc.[principal\_id] = members.[role\_principal\_id]

JOIN

--Role members (database users)

sys.database\_principals memberprinc ON memberprinc.[principal\_id] = members.[member\_principal\_id]

LEFT JOIN

--Login accounts

sys.login\_token ulogin on memberprinc.[sid] = ulogin.[sid]

LEFT JOIN

--Permissions

sys.database\_permissions perm ON perm.[grantee\_principal\_id] = roleprinc.[principal\_id]

LEFT JOIN

--Table columns

sys.columns col on col.[object\_id] = perm.major\_id

AND col.[column\_id] = perm.[minor\_id]

LEFT JOIN

sys.objects obj ON perm.[major\_id] = obj.[object\_id]

UNION

--List all access provisioned to the public role, which everyone gets by default

SELECT

[UserName] = '{All Users}',

[UserType] = '{All Users}',

[DatabaseUserName] = '{All Users}',

[Role] = roleprinc.[name],

[PermissionType] = perm.[permission\_name],

[PermissionState] = perm.[state\_desc],

[ObjectType] = obj.type\_desc,--perm.[class\_desc],

[ObjectName] = OBJECT\_NAME(perm.major\_id),

[ColumnName] = col.[name]

FROM

--Roles

sys.database\_principals roleprinc

LEFT JOIN

--Role permissions

sys.database\_permissions perm ON perm.[grantee\_principal\_id] = roleprinc.[principal\_id]

LEFT JOIN

--Table columns

sys.columns col on col.[object\_id] = perm.major\_id

AND col.[column\_id] = perm.[minor\_id]

JOIN

--All objects

sys.objects obj ON obj.[object\_id] = perm.[major\_id]

WHERE

--Only roles

roleprinc.[type] = 'R' AND

--Only public role

roleprinc.[name] = 'public' AND

--Only objects of ours, not the MS objects

obj.is\_ms\_shipped = 0

ORDER BY

princ.[Name],

OBJECT\_NAME(perm.major\_id),

col.[name],

perm.[permission\_name],

perm.[state\_desc],

obj.type\_desc--perm.[class\_desc]