

## Re: (Newbie)Application Roles

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-08/0427.html>

---

**From:** Michael Shao [MSFT] ([v-yshao\\_at\\_online.microsoft.com](mailto:v-yshao_at_online.microsoft.com))

**Date:** 08/20/03

Date: Wed, 20 Aug 2003 16:21:47 GMT

Hi Lars,

Thanks for Vinod's help. The name of the application role does not need to be the same name as the application. There is not obvious relationship between them.

The security system in Microsoft® SQL Server™ is implemented at the lowest level: the database itself. This is the best method for controlling user activities regardless of the application used to communicate with SQL Server. However, sometimes security controls must be customized to accommodate the special requirements of an individual application, especially when dealing with complex databases and databases with large tables.

Additionally, you may want users to be restricted to accessing data only through a specific application (for example using SQL Query Analyzer or Microsoft Excel) or to be prevented from accessing data directly. Restricting user access in this way prohibits users from connecting to an instance of SQL Server using an application such as SQL Query Analyzer and executing a poorly written query, which can negatively affect the performance of the whole server. SQL Server accommodates these needs through the use of application roles. The fundamental differences between standard and application roles are:

- Application roles contain no members. Users, Microsoft Windows NT(r) groups, and roles cannot be added to application roles; the permissions of the application role are gained when the application role is activated for the user's connection through a specific application(s).

A user's association with an application role is due to being capable of running an application that activates the role, rather than being a member of the role.

- Application roles are inactive by default and require a password to be activated by using the `sp_setapprole` system stored procedure. The password can be provided by the user, for example, through an application prompt, but it is more likely that the password is incorporated within the

application. The password can be encrypted as it is sent to SQL Server.

– When an application role is activated for a connection by the application, the connection permanently loses all permissions applied to the login, user account, or other groups or database roles in all databases for the duration of the connection. The connection gains the permissions associated with the application role for the database in which the application role exists. Because application roles are applicable only to the database in which they exist, the connection can gain access to another database only by virtue of permissions granted to the guest user account in the other database. Therefore, if then guest user account does not exist in a database, the connection cannot gain access to that database. If the guest user account does exist in the database but permissions to access an object are not explicitly granted to guest, the connection cannot access that object regardless of who created the object. The permissions the user gained from the application role remain in effect until the connection logs out of SQL Server.

For additional information regarding the application role, please refer to the following article:  
243053 HOWTO: Create an Application Role on Microsoft SQL Server 7.0  
<http://support.microsoft.com/?id=243053>

Also I have found the related article in SQL Server Books Online below:  
Topic: "Establishing Application Security and Application Roles"

Hope it helps

Regards,

Michael Shao  
Microsoft Online Partner Support  
Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)  
This posting is provided "as is" with no warranties and confers no rights.