

Re: SQL Access security from Window Application

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.general/2005-09/msg00562.html>

- *From:* "Mary Chipman [MSFT]" <mchip@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Sep 2005 14:30:54 -0400
-

Yes, you could have your app handle authentication by emulating the way web applications work, storing users, groups, and passwords in tables in a separate database. If the user is validated, then they get to connect, if not, then no. Your app would then use a single login to connect to the real SQLS database, which individual users wouldn't have access to. This would simplify granting EXEC perms on the stored procedures because you'd only have one login/user to contend with (also good for pooling). If different levels of access are required, then you could also control this from your validation app. This would be a lot of work to set up, but easier to maintain and possibly more secure, since users would not be able to connect at all on their own and you'd configure the logins the app uses to not have elevated permissions. Take a look at <http://msdn.microsoft.com/library/en-us/dnnetsec/html/secnetlpMSDN.asp> — there's a chapter on data access security that you could repurpose.

--Mary

On Thu, 8 Sep 2005 10:13:38 -0400, "John J. Hughes II" <no@xxxxxxxxxxxx> wrote:

>I am having some major problem with maintaining security for my windows
>application to the SQL. Currently my application access the SQL using
>System.Data.SqlClient and all forms use stored procedures. It seems the
>preferred method is to restrict access to all table and then to set the
>execute option based on each stored procedure and handle the error in some
>intelligent way. Now this is causing several problems the first being
>setting the correct access on the several hundred stored procedures and the
>second being changing each user access whenever a new stored procedure is
>added. Both are becoming maintenance nightmares.
>
>Now I would prefer to set the permission in my application and save the
>passwords in a protected file but this creates a problem on remote systems
>whereas the passwords can't be set from a central location so I don't see it
>as feasible.
>
>I was thinking of creating a small service that could run on a central
>server to verify passwords and instruct my application on how to set behave

Re: SQL Access security from Window Application

>but this does not stop the user from just bypassing my application and
>access the SQL directly. The preferred method would be not to allow them
>access to the SQL at all but have my program act as a conduit which would
>handle the security. But I am not sure how feasible this is. The other
>option would be for the service to verify the user name against the SQL and
>send the correct login to the application. This would at least hide the
>login data assuming a secure connect.

>
>Does anyone know of a better way of handling this?

>
>Regards,
>John

>

.

- *Follow-Ups:*

- ◆ [Re: SQL Access security from Window Application](#)

- ◇ *From:* John J. Hughes II

- *References:*

- ◆ [SQL Access security from Window Application](#)

- ◇ *From:* John J. Hughes II

- Prev by Date: [Setup Projects and .lnk Shortcuts](#)
- Next by Date: [Visual Studio.Net trial and Frameworks 2.0](#)
- Previous by thread: [SQL Access security from Window Application](#)
- Next by thread: [Re: SQL Access security from Window Application](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)