

RE: Combine Forms Authentication with Windows

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.general/2005-11/msg00185.html>

- *From:* stcheng@xxxxxxxxxxxxxxxxxxxxxx (Steven Cheng[MSFT])
 - *Date:* Tue, 08 Nov 2005 11:56:53 GMT
-

Hi Nick,

Have you got any further ideas on this question or does the things in my last reply helps a little? If there're anything else we can help, please feel free to post here. Thanks,

Steven Cheng
Microsoft Online Support

Get Secure! www.microsoft.com/security
(This posting is provided "AS IS", with no warranties, and confers no rights.)

| X-Tomcat-ID: 182654618
| References: <96F85096-EC47-4F6B-AA95-75C313F4E19F@xxxxxxxxxxxxxx>
<20F3E20C-36C0-4647-ABBD-8214A5365DF9@xxxxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain
| Content-Transfer-Encoding: 7bit
| From: stcheng@xxxxxxxxxxxxxxxxxxxxxx (Steven Cheng[MSFT])
| Organization: Microsoft
| Date: Fri, 04 Nov 2005 10:04:51 GMT
| Subject: RE: Combine Forms Authentication with Windows
| X-Tomcat-NG: microsoft.public.dotnet.general
| Message-ID: <IvRu8cS4FHA.2984@xxxxxxxxxxxxxxxxxxxxxx>
| Newsgroups: microsoft.public.dotnet.general
| Lines: 119
| Path: TK2MSFTNGXA01.phx.gbl
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.dotnet.general:53498
| NNTP-Posting-Host: tomcatimport2.phx.gbl 10.201.218.182

| Thanks for Rainier's inputs.

| Hi Nick,

| As for your scenario, I'm afraid it's quite hard to meet all your
| requirement. Since you'd like to make the authenticaiton transparent to
| client user, of course using FormsAuthentication (anonymous access in

RE: Combine Forms Authentication with Windows

IIS)

| should be choosed. However, since those internal users need to call
| protected store procedures on remote SQLserver under their windows
| identity, we have to programmatically impersonate them (throw clear text
| username /password) in code when necessary. I think this is also what
you

| currently thinking, yes?

| Also, another means is we move the protection of those store procedures
out
| of the SQLSERVER's buildin role based checking, and check the caller's
| account in our code. In other word, we make no protection for those store
| procedures in SQLSERVER so that any upstream callers and call them. And
| what we need to do is checking the clientuser in our code (in the web
| application's data accessing component ...)

| So far I think we have the above two approachs. Just my opinion.

| Thanks,

| Steven Cheng
| Microsoft Online Support

| Get Secure! www.microsoft.com/security
| (This posting is provided "AS IS", with no warranties, and confers no
| rights.)

|-----
|| Thread-Topic: Combine Forms Authentication with Windows
|| thread-index: AcXhIVpRkjMtDNpSTZGoEkqs/ZYaw==
|| X-WBNR-Posting-Host: 195.50.100.20
|| From: "=?Utf-8?B?UmFpbmllciBbTUNUXQ==?=" <RainierMCT@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
|| References: <96F85096-EC47-4F6B-AA95-75C313F4E19F@xxxxxxxxxxxx>
|| Subject: RE: Combine Forms Authentication with Windows
|| Date: Fri, 4 Nov 2005 01:23:01 -0800
|| Lines: 46
|| Message-ID: <20F3E20C-36C0-4647-ABBD-8214A5365DF9@xxxxxxxxxxxx>
|| MIME-Version: 1.0
|| Content-Type: text/plain;
|| charset="Utf-8"
|| Content-Transfer-Encoding: 7bit
|| X-Newsreader: Microsoft CDO for Windows 2000
|| Content-Class: urn:content-classes:message
|| Importance: normal
|| Priority: normal
|| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.0
|| Newsgroups: microsoft.public.dotnet.general
|| NNTP-Posting-Host: TK2MSFTNGXA03.phx.gbl 10.40.2.250

RE: Combine Forms Authentication with Windows

|| Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGXA03.phx.gbl
|| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.dotnet.general:53496
|| X-Tomcat-NG: microsoft.public.dotnet.general

||
|| It's quite a story you wrote.
|| You do not want users to be authenticated by the database by using a
|| username password, because this means that every user will get its own
|| connection.

||
|| So you need integrated security, this means that the users need
|| NT-Credentials(Kerberos/NTLM). So you will need to use integrated
|| security

|| and
|| impersonation for the authenticated users.

||
|| For the non authenticated users, you will need to use a second
|| connectionstring one that uses the credentials given to the application
|| (aspnet user by default)

||
|| Give less rights to these anonymous users.

||
|| Hope I answered the right question...

||
|| Good luck,

|| ---
|| Rainier van Slingerlandt
|| (Freelance trainer/consultant/developer)
|| www.slingerlandt.com

||
|| "Nick" wrote:

||
|| > I am working a new application...well actually a series of
|| applications
|| for
|| > my company. They want internal users to be able to go to a site and
|| > everything regarding security is transparent, however we will have
|| brokers
|| > and customers that also need to connect and will require a username
|| and
|| > password. In this case we were going to store their credentials in a
|| SQL
|| > database. Internal users will have the ability to access the same
|| resources
|| > as the external brokers and customers. Is there an easy way that I
|| can
|| > combine both methods? Internal users would go off of Active
|| Directory
|| > security groups for security roles, and external users would go off a
|| > internal roles database table. I was told that nothing should be set
|| in a

RE: Combine Forms Authentication with Windows

|| > web.config file for roles and users. I have seen in ASP.NET how to
|| > impersonate a user in code, but would that really be the best
solution
| in
|| > this case as it would be done quite a bit? In order for transparent
| security
|| > for users I could easily use forms authentication with cookies that
| save. As
|| > for SQL security if I must use strictly forms authentication and have
a
|| > general database login that works for all web applicaitons I could
| secure it
|| > by allowing stored procedures only and deny everything else. How
could
| I
|| > then secure users from accessing procedures if there is a bug in the
|| > application. Is there a way that I can prevent users in my users
table
| from
|| > calling certain procedures? Thanks for anyone's input.
||
|
|

-
- Prev by Date: [*datagrid current row*](#)
 - Next by Date: [*Group similar taskbar buttons in the Taskbar doesn't work \(C# solution \) ?*](#)
 - Previous by thread: [*datagrid current row*](#)
 - Next by thread: [*Group similar taskbar buttons in the Taskbar doesn't work \(C# solution \) ?*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)