

## Re: server authentication & ASP authentication

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2002-07/1132.html>

---

**From:** Jakub Jablonski ([jakubjab@data.pl](mailto:jakubjab@data.pl))

**Date:** 07/06/02

Date: Sat, 06 Jul 2002 01:40:21 +0200  
From: Jakub Jablonski <[jakubjab@data.pl](mailto:jakubjab@data.pl)>

Aaron,

This is all intranet, but some day it may be internet also. We use different versions of Windows, Unix, Linux and all sorts of browsers as clients.

The SQL Server and web server are on the same machine (Windows 2000).

Let me make sure I understood correctly your suggestion:

1. Create Windows account for each employee and the local group for each group of employees on the machine where IIS and SQL Server run.
2. Disable Anonymous and enable Basic authentication and SSL on the web server (Integrated Windows doesn't work with Netscape, am I correct?)
3. Use windows instead of standard authentication on SQL Server. Do I also need to create a server login and a database user for each employee? Does it affect performance to have 120 logins in SQL Server?

Then the sequence is (correct me if I'm wrong):

- employee opens web browser and sends request to the IIS.
- IIS responses with the request for basic authentication
- employee enters his/her login and password
- IIS accepts credentials and runs the ASP application under that user's context
- ASP application connects to the SQL Server using connection string without password
- SQL Server recognizes the user and grants him/her appropriate permissions.

I guess I can find the login name in ServerVariables. What is the difference between AUTH\_USER, LOGON\_USER and REMOTE\_USER variables in my case? How to find the group of the user?

How can I prevent users from logging in directly to the machine where they have accounts, and use only the web application?

Thank you for the answer  
Regards,  
Jakub Jablonski

Aaron Margosis [MS] wrote:

- > *Is this all intranet? If not, is there a firewall between your web server*
- > *and database? Are the web server and DB on the same machine?*
- >
- > *My primary inclination would be to use platform authentication across the*
- > *board. That is, create Windows accounts for each of the 120 users. Use*
- > *Integrated Windows or Basic authentication on the web server (disallow*
- > *anonymous access), and Windows authentication to the database. This does a*
- > *number of things for you that you would otherwise have to do in code:*
- > *\* Secure management of credentials. Passwords are hashed, rather than*
- > *stored in clear text (the original password cannot be derived from the*
- > *hash). The hashes are accessible only to the OS. A user's password can be*
- > *changed only by the user or an administrator. It is also easy to enforce*
- > *password complexity, password expiration, and account lockout after a*
- > *specified number of unsuccessful attempts.*
- > *\* With Integrated Windows (NTLM or Kerberos), passwords are not transmitted*
- > *over the network in the clear. With Basic authentication, add SSL to*
- > *achieve the same.*
- > *\* EVERY entry point to your application and database enforces authentication*
- > *and authorization.*
- > *\* Validation checks are performed correctly every time.*
- > *\* Subsequent requests in the same user session are correctly associated with*
- > *the initial authentication. You don't need to set/get encrypted cookies to*
- > *determine who the user is.*
- >
- > *With SQL Server, it is easy to map Windows groups to roles. Groups can be*
- > *defined locally -- you don't need them to be established at the domain*
- > *(although you could do that too).*
- >
- > *Embedding passwords in text files on the hard drive is not secure --*
- > *especially if the file lives at or under your web application's vroot.*
- > *There have been vulnerabilities in the past that allow an attacker's request*
- > *for a specific file (e.g., a .asp page) to download the raw file rather than*
- > *run it on the server. (In other words, a user could download the asp page*
- > *that contains the username/password.)*
- >
- > *HTH*
- >
- > *-- Aaron*