Visual Basic and Visual C# Concepts

Accessing SQL Server Using Windows Integrated Security

If your application runs on a Windows-based intranet, you might be able to use Windows integrated security for database access. Integrated security requires:

- That SQL Server is running on the same computer as IIS.
- That all application be users on the same domain so that their credentials are available to the Web server. (That is, Windows integrated security is not practical for a public Web site.)

To access SQL Server using Windows integrated security, you need to configure four different areas of your application:

- IIS
- The application configuration file (Web.config)
- Connection strings
- SQL Server itself

Configuring IIS

You need to configure your application in IIS to turn off anonymous access and turn on Windows authentication.

To configure IIS for Windows integrated security

1. In Windows, open the Internet Information Services administration tool.
    - In Windows 2000, this is available from the Start menu by pointing to Programs, then Administrative Tools, and then Internet Services Manager.
    - In Windows XP, this is available from Administrative Tools in the Control Panel.
2. Open the node for your server, and then open nodes until you find the node for your application, typically under Default Web Site.
3. Right-click your application and choose **Properties**.
4. In the **Directory Security** tab, click **Edit**.
5. In the **Authentication Methods** dialog box, clear the **Anonymous Access** box and make sure **Integrated Windows authentication** is checked.
6. Click **OK** to close all the dialog boxes.

Configuring the Web.config File

In the application configuration file (Web.config), you establish the authentication mode that your application uses and establish that the application will impersonate the user's credentials — that is, that it will run as that user.

To configure Web.config to allow Windows integrated security

- Open the Web.config file for your application and add the following elements to it:

-
  ```
  <authentication mode="Windows" />
  ```

  ```
  <identity impersonate="true"/>
  ```

  The <authentication> element might already be there.

  Note Elements in Web.config are case sensitive.

Creating Connection Strings

When you create a connection string to access SQL Server, you must include attributes that tell SQL Server that you are using Windows integrated security.

To configure connection strings for Windows integrated security

- In any connection string for SQL Server, include the attribute `Trusted_Connection=Yes` and remove the username and password attributes.

  The following shows a typical connection string configured for Windows integrated security:

  ```
  "workstation id=WebServer1;packet size=4096;
  Trusted_Connection=Yes;data source=mySqlServers";
  persist security info=False;initial catalog=northwind"
  ```

Configuring SQL Server

You must set up SQL Server to recognize the users who will be accessing it.

To configure SQL Server for Windows integrated security

1. From the Windows **Start** menu, choose **Microsoft SQL Server**, and then choose **Enterprise Manager**.
2. Open the node for the server and expand the node for the database you want to give users permissions for.
3. Right-click the **Users** node and choose **New Database User**.
4. In the **Database User Properties** dialog box, enter *domain**username* in the **Login name** box, and then click **OK**. Alternatively, configure the SQL Server to allow all domain users to access the database.