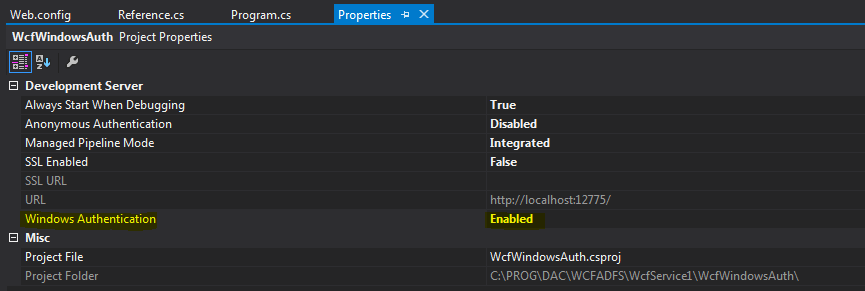
Allowing specific users to use a WCF web service

As the title suggest this procedure does not cover all of the things that we can do to secure access to a WCF web service, for example, you may want some users to have access to different method while some won’t or may want to encrypt the communication. You WILL NOT find these answers here. In fact this procedure should be used in an environment where you want to allow only specific users to access your web service and once they have access to it, they have access to everything. It can also be used in an environment where the web service is highly used. This procedure applies specifically to WCF Service Application

Enabling Windows authentication

The allow Windows Authentication. (F4 on the project name, in the solution explorer)



Add the following to Web.Config

|  |
| --- |
| <?xml version="1.0"?>  <configuration>  <system.web>  <authentication mode="Windows"/>  <authorization>  <allow users="?"/>  </authorization> |

Note:

Allow users=”?” specify anonymous

So let’s say you want to allow someone you would type something like :

|  |
| --- |
| <allow users="canamgroup\erictalb"/> |

Ref: <http://msdn.microsoft.com/en-us/library/acsd09b0%28v=vs.85%29.aspx>

Bindings

My intention here is not to specify how to define bindings, but only to bring to your attention that within the bindings you must define the Security Mode to TransportCredentialOnly and Transport clientCredentialType to Windows. This way the WCF web service will use Windows authentication to authenticate windows users.

|  |
| --- |
| <bindings>  <basicHttpBinding>  <binding name="BasicHttpEndpointBinding">  <security mode="TransportCredentialOnly">  <transport clientCredentialType="Windows" />  </security>  </binding>  </basicHttpBinding>  </bindings> |

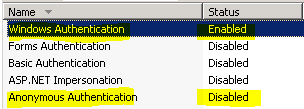
Then bind the interface to the bindings

|  |
| --- |
| <services>  <service behaviorConfiguration="WcfWindowsAuth.Service1Behavior" name="WcfWindowsAuth.Service1">  <endpoint address="http://test\_adfswcf.canam.ws/service1.svc" binding="basicHttpBinding" bindingConfiguration="BasicHttpEndpointBinding" name="BasicHttpEndpointBinding" bindingNamespace="WcfWindowsAuth" contract="WcfWindowsAuth.IService1">  </endpoint>  </service>  </services> |

Hosting on IIS

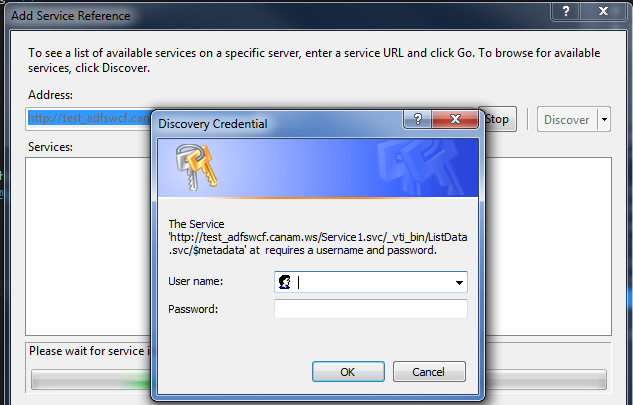
Hosting on a server requires a few extra steps as we have to enable windows authentication on the web site.





Consuming the service.

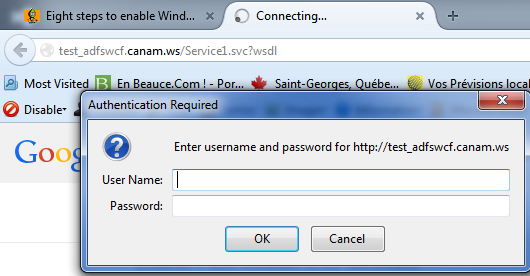
Could not be easier, adding a reference to the service will automatically use you current windows logged user and if you are not in the allow statement, you will get the following:



Notice that you don’t need to set extra logging information in your code, it is implied that the current windows user will be used to authenticate against the WCF web service.

|  |
| --- |
| class Program  {  static void Main(string[] args)  {  ServiceReference1.Service1Client obj = new ServiceReference1.Service1Client();  Console.WriteLine(obj.GetData(1));    }  }  } |

Finally, if you try to access to WCF web service from anywhere else using a NON-ALLOWED windows user you get a login window



Full WEB.config listing here:

|  |
| --- |
| <?xml version="1.0"?>  <configuration>  <appSettings>  <add key="aspnet:UseTaskFriendlySynchronizationContext" value="true" />  </appSettings>  <system.web>  <compilation debug="true" targetFramework="4.5" />  <httpRuntime targetFramework="4.5"/>  <authentication mode="Windows"/>  <authorization>  <allow users="canamgroup\erictalb"/>  </authorization>  </system.web>  <system.serviceModel>  <bindings>  <basicHttpBinding>  <binding name="BasicHttpEndpointBinding">  <security mode="TransportCredentialOnly">  <transport clientCredentialType="Windows" />  </security>  </binding>  </basicHttpBinding>  </bindings>  <services>  <service behaviorConfiguration="WcfWindowsAuth.Service1Behavior" name="WcfWindowsAuth.Service1">  <endpoint address="http://test\_adfswcf.canam.ws/service1.svc" binding="basicHttpBinding" bindingConfiguration="BasicHttpEndpointBinding" name="BasicHttpEndpointBinding" bindingNamespace="WcfWindowsAuth" contract="WcfWindowsAuth.IService1">  </endpoint>  </service>  </services>  <behaviors>  <serviceBehaviors>  <behavior name="WcfWindowsAuth.Service1Behavior">  <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true"/>  <serviceDebug includeExceptionDetailInFaults="false"/>  </behavior>  </serviceBehaviors>  </behaviors>  <protocolMapping>  <add binding="basicHttpsBinding" scheme="https" />  </protocolMapping>  <serviceHostingEnvironment aspNetCompatibilityEnabled="true" multipleSiteBindingsEnabled="true" />  </system.serviceModel>  <system.webServer>  <modules runAllManagedModulesForAllRequests="true"/>  <directoryBrowse enabled="true"/>  </system.webServer>  </configuration> |