# Install Solution and Feature Activation

## Purpose:

The solution installation will put the provider DLL in your server GAC and activating its features will insert the proper entries in your web.config files.

## Prepare External References

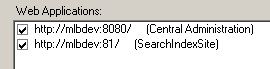
This membership provider relies on external files to write web.config entries and handle ULS logging. Before installing this solution, you will need to prep your server with these external files. You may do so by either dropping their .dlls into your server’s GAC or by running their individual installs (both are packaged as solution files).

ULS Logger- at [My Local Broadband Community Projects](http://www.codeplex.com/MyLocalBroadband/Wiki/View.aspx?title=ULS%20Logger)

Web Config Manager-at [My Local Broadband Community Projects](http://www.codeplex.com/MyLocalBroadband/Wiki/View.aspx?title=Web%20Config%20Manager)

## Procedure:

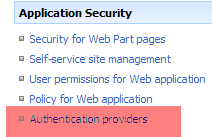
1. Run Setup.exe
2. Click next until you get to the screen where it asks for the deployment targets. Here Click your central admin application and the web application where you want to enable the security provider.



1. Click next and finish the installation.
2. Open Central Administration and Go to the Application Management Tab.
3. Click the Manage Web Application Features link
4. For Your Central Administration V3 web application, activate the “My Local Broadband LLC – Security Provider Web Services”
5. Then select the web application where you want to use the Security Provider (Forms Based Authentication). In this web application, activate the feature, “My Local Broadband LLC – WSS Security Provider”.
6. Correct the web.config keys if necessary. See Appendix A. (appendix A, pretty official sounding eh?)

Now we need to configure Forms Based Authentication.

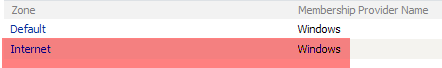
1. In the Central Administration Application Management Tab, click the Authentication Providers link.



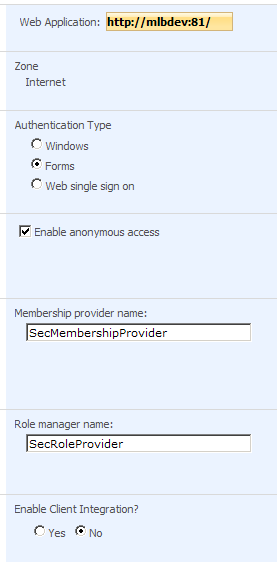
1. Choose the Web Application where you want to configure FBA.



1. Then click on the zone where you want to enable FBA. In this example I have extended my default zone and want to configure FBA on the Internet Zone.



1. Click the Forms radio button for Authentication Type.
2. Check Enable Anonymous Access (if desired)
3. Enter SecMembershipProvider for Membership provider name (adjust to your web.config entry if you altered these from the original values in my solution.
4. Enter SecRoleProvider for Role manager name (adjust to your web.config entry if you altered these from the original values in the solution.
5. Client integration gives mixed results with FBA, so pick a value that suits your situation.



1. Click Save

# Appendix A

If you kept the default database name and your SQL Server is the default instance on your web server, you may not need to continue. Otherwise you will now need to adjust the web.config for your web applications. You will need to correct this in all web.config files associated with the activated features, which will be in at least two places, your central administration web app and your intended FBA web app. In addition, if you are extending a windows authenticated web app into an FBA web app, you will want to correct it in both places.

You may want to change this in the source code and just compile a version that is correct in your environment.

The keys inserted in the FBA web app’s web.config are:

<membership defaultProvider="SecMembershipProvider">

<providers>

<add name="SecMembershipProvider" connectionStringName="SecProviderConnectionString" enablePasswordRetrieval="false" enablePasswordReset="true" requiresQuestionAndAnswer="false" applicationName="SecProviderFormsAuth" requiresUniqueEmail="false" passwordFormat="Hashed" maxInvalidPasswordAttempts="5" minRequiredPasswordLength="1" minRequiredNonalphanumericCharacters="0" passwordAttemptWindow="10" passwordStrengthRegularExpression="" type="MyLocalBroadband.WSSSecurityProvider.SqlSiteMembershipProvider, MyLocalBroadband.WSSSecurityProvider, Version=1.0.0.0, Culture=neutral, PublicKeyToken=af1a525c93de384c" />

</providers>

</membership>

<roleManager defaultProvider="SecRoleProvider" enabled="true">

<providers>

<add name="SecRoleProvider" connectionStringName="SecProviderConnectionString" applicationName="SecProviderFormsAuth" type="MyLocalBroadband.WSSSecurityProvider.SqlSiteRoleProvider, MyLocalBroadband.WSSSecurityProvider, Version=1.0.0.0, Culture=neutral, PublicKeyToken=af1a525c93de384c" />

</providers>

</roleManager>

<connectionStrings>

<add name="SecProviderConnectionString" connectionString="data source=127.0.0.1;Integrated Security=SSPI;Initial Catalog=SecProviderDB" />

</connectionStrings>

The Central Administration’s web.config gets these keys.

<membership defaultProvider="SecMembershipProvider">

<providers>

<add name="SecMembershipProvider" connectionStringName="SecProviderConnectionString" enablePasswordRetrieval="false" enablePasswordReset="true" requiresQuestionAndAnswer="false" applicationName="SecProviderFormsAuth" requiresUniqueEmail="false" passwordFormat="Hashed" maxInvalidPasswordAttempts="5" minRequiredPasswordLength="1" minRequiredNonalphanumericCharacters="0" passwordAttemptWindow="10" passwordStrengthRegularExpression="" type="System.Web.Security.SqlMembershipProvider" />

</providers>

</membership>

<roleManager defaultProvider="SecRoleProvider">

<providers>

<add name="SecRoleProvider" connectionStringName="SecProviderConnectionString" applicationName="SecProviderFormsAuth" type="System.Web.Security.SqlRoleProvider" />

</providers>

</roleManager>

<connectionStrings>

<add name="SecProviderConnectionString" connectionString="data source=127.0.0.1;Integrated Security=SSPI;Initial Catalog=SecProviderDB" />

</connectionStrings>

The keen eye may see that the FBA web app’s web.config gets membership and role providers that point to our custom provider, while the central administration’s web.config gets keys that point at the standard sql providers. That’s because our web services need access to the provider database, but we won’t be hitting these web services from the hosted FQDN. We’ll handle the translation to the correct provider application name (FQDN) in the code by handing in the appropriate FQDN as a parameter in the web service calls.

In addition, your Central Administration’s web.config will get the following key that points to the local hosts file. Make sure it has the correct path for the associated web service calls to work.

<appSettings>

<add key="HostsFile" value="C:\Windows\system32\drivers\etc\hosts" />

</appSettings>