# Purpose

This paper will walk you through setting up a single server (small farm) installation with a working hosted-style configuration complete with working search. The problem, [described here](http://technet.microsoft.com/en-us/library/cc287830.aspx), is that indexing cannot be done on a forms based authentication web application, it must use windows (NTLM) authentication. This is further complicated here because we will be using host headers to bring users into our sites using fully qualified domain names. When host header mode is used, then the site url as it is indexed must exactly match the site url as the user browses.

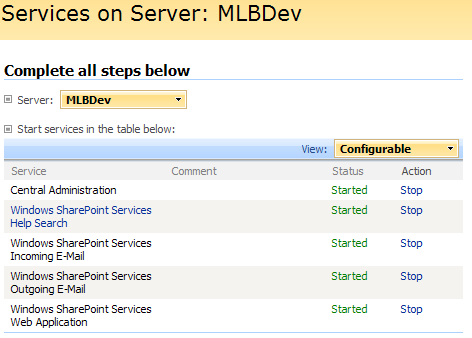
You can probably read through that article and figure this stuff out, but this paper will detail a working example using this solution. This example works, but be warned: troubleshooting issues with search is a real bitch. Believe me. This is my 3rd or 4th incarnation of this paper because in each of the earlier versions I made some small change along the way that caused indexing to fail in the end.

# Overview

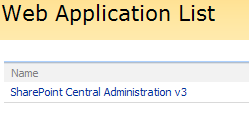
We’ll create a two web applications that listen to port 80. The default zone will use our FBA provider and run on all unassigned IP addresses, the Intranet zone will use NLTM authentication and run only on port 127.0.0.1.

# Initial State

* This is a single server set up as a small farm installation for WSS 3.0 (not MOSS).
* The services are already configured and running. This one has incoming and outgoing email set up, but that is not necessary for this demo.



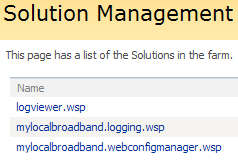
* The only web application set up is the Central Admin web app.



* Also, there are no other IIS sites running on the server



* This server has three solutions already installed, but none is necessary at this point
  + The logviewer.wsp is available here: <http://www.codeplex.com/features> it is a handy utility that lets you view and filter the ULS from within Central Administration.
  + The two mylocalbroadband solutions are needed for this solution to function and their installation point will be called out later in these instructions.



# Procedure

## Create a new web application in Central Administration

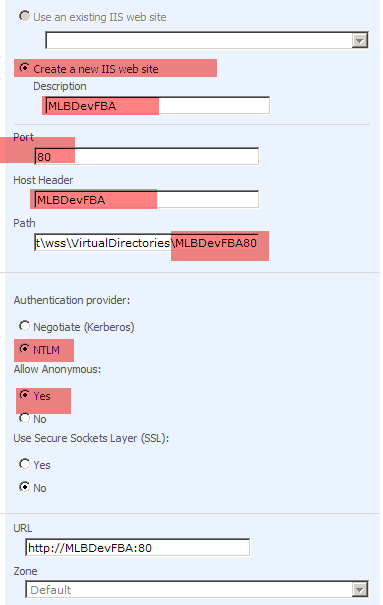
1. In the central administration’s application tab, click Create or extend Web application.

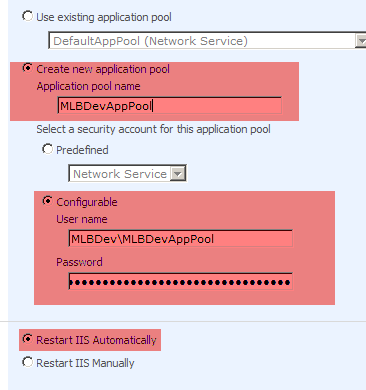


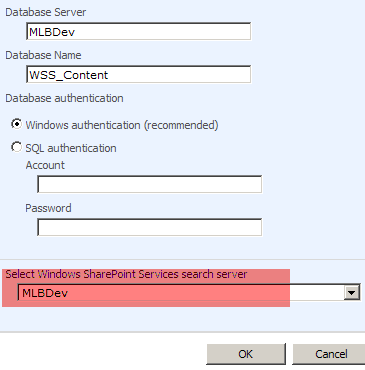
1. Click Create a new Web application



1. Fill in the values and hit OK. My changes from the defaults are highlighted here. For the app pool account, make sure you use a valid username/password on your system.







* + Your web application list will now look similar to this:



## Create your Intranet zone

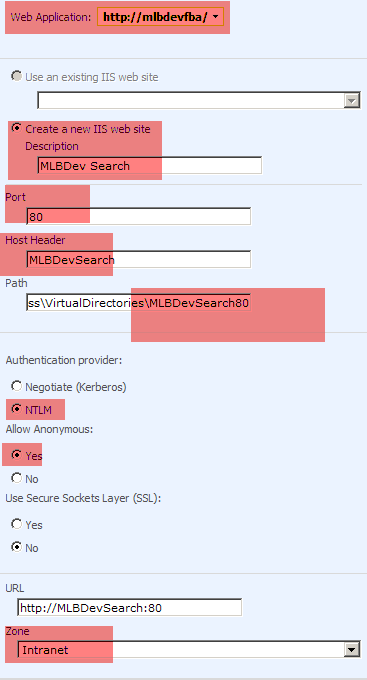
1. In the central admin’s application tab, click create or extend web application



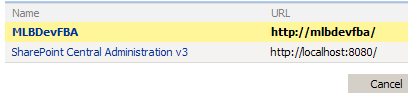
1. Click Extend an existing Web application



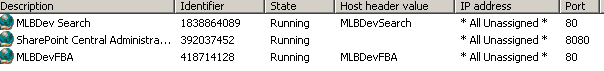
1. Fill in the values to extend your previous web app onto port 80. My changes from the default are highlighted here:



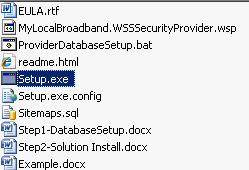
1. Hit OK
2. Your Web application list will still look like this:



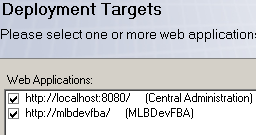
And if you look in your IIS manager, you should see something like this:



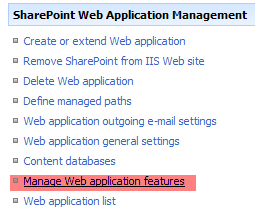
1. Install the necessary Solutions from the [My Local Broadband Community Projects](http://www.codeplex.com/MyLocalBroadband/)
   * Install the ULS Logger
   * Install the Web Config Manager
   * Install the WSS Security Provider – **Note: there is overlap between these instructions and the ones in the setup documents. If you read through them both, you will see how they fit together. There are steps in the setup document that are not explained here. For example, you will need to set up the provider database and may need to correct the web.config keys to your situation. Instructions for these steps are in the set up documentation.**
     1. Use the setup.exe



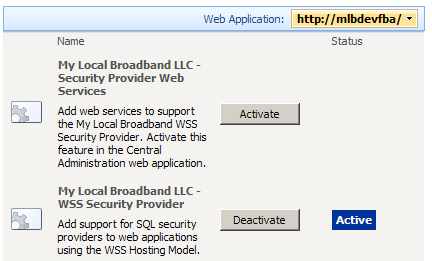
* + 1. At the deploy targets screen, choose both central admin and your dev fba web applications.



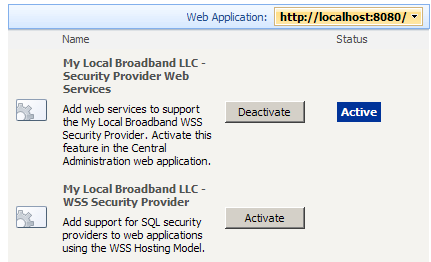
* + 1. Open the application management tab in central admin.
    2. Click the manage web application features link.



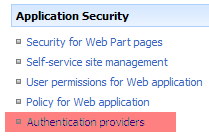
* + 1. For your fba web app, activate the My Local Broadband LLC – WSS Security Provider feature



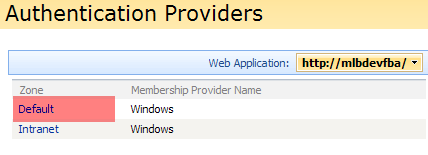
* + 1. For your central admin web app, activate the My Local Broadband LLC – Security Provider Web Services feature.



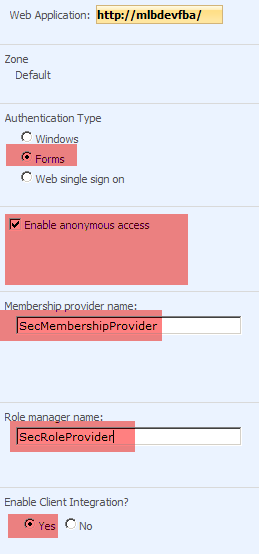
1. We’ll now activate the forms authentication provider. Go to the application management tab of central administration again and click the Authentication providers link.



1. Make sure you are looking at the correct web application and then click the Internet zone link



1. Set up the values as highlighted here and then click Save.



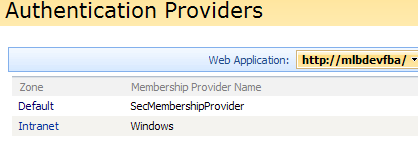
**A note on Anonymous Access:**

Checking this Enable anonymous access box does not enable anonymous access for all sites collections within the application. Instead, it activates the possibility of anonymous access within the application’s site collections. So you’ll want to check it at this level and then actually control it at an individual site level.

**A note on Client Integration:**

Client integration is not without problems with Forms Based Authentication. However, as long as you enable the remember me checkbox on logins, the Office programs work well and probably make it worthwhile to enable the integration here. See the end of this article for notes on making remember me work correctly.

1. You’ll then see the intranet zone set up with the membership provider name.

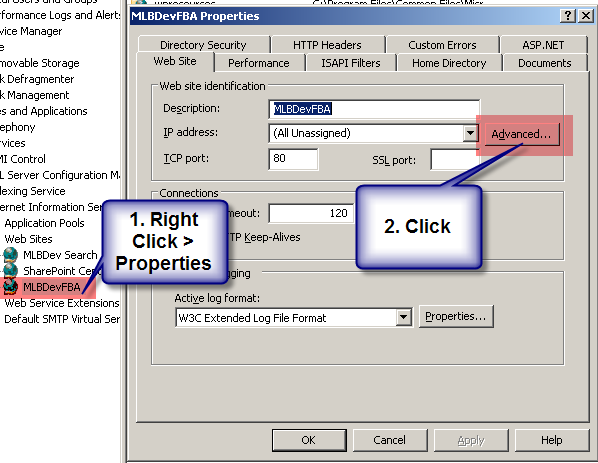


## Make FBA Response on all IPs

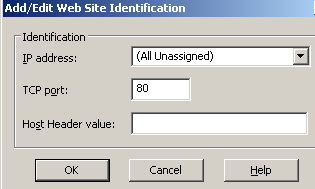
1. Open your IIS Manager and navigate to your IIS web Applications

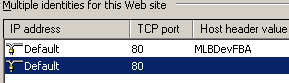


1. Central admin added a host header entry to our IIS site properties, but we want to add an additional entry that is not bound to a host header.
2. Go to the Host-FBA app’s properties.
3. In the Web site tab, click the advanced button.



1. Then click the add button and add an entry where port is 80 and ip is all unassigned.

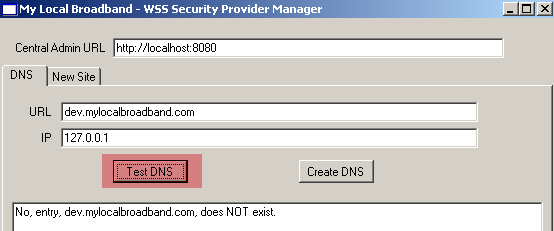


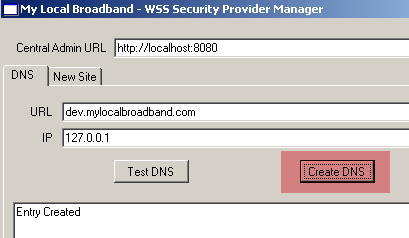


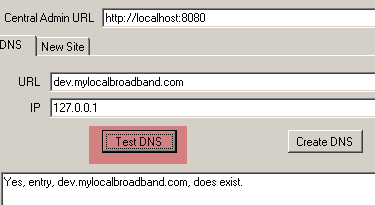
1. Click Ok until you are back at the IIS Manager.

## Create your FQDN site

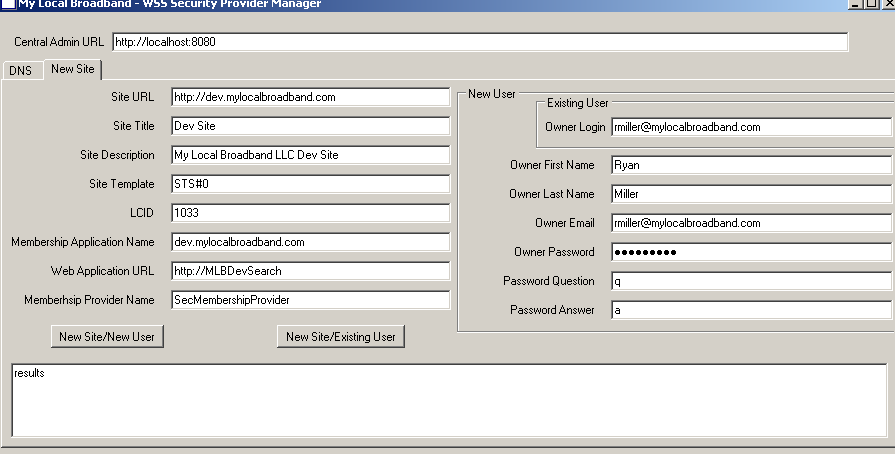
1. Fire up the client: MyLocalBroadband.WSSSecurityManagement.Client.exe
2. Create a DNS (Hosts file) entry using the DNS tab of the client. NOTE: if you’re using an actual DNS server, you can make this record entry there.







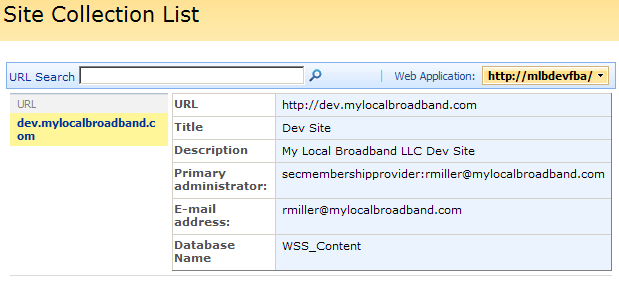
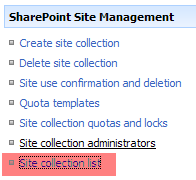
1. You’ll want to create entries for both your web app host headers, and your search machine name as well as your site’s FQDN. For me, this translates into host header entries for mlbdev, mlbdevfba, mlbdevsearch, and dev.mylocalbroadband.com.
2. Now switch over to the New Site tab.



1. Fill in your values as chosen and click the New Site/New User button.

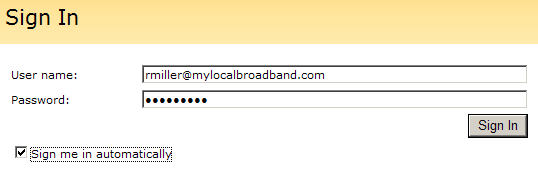


1. If all goes well, after a few seconds, you should see the results box display “Site and User Created”. If there is a failure, you’ll see the exception displayed in the results box.
2. You can also go to the site collection list (central admin applications tab) and see that your site is created in the correct web application.

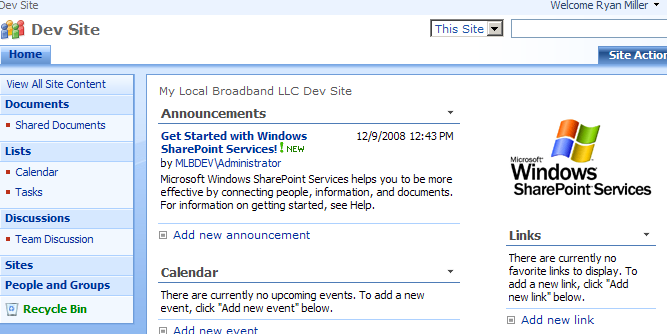


## Test FBA

1. Since our MLBDevFBA application was configured to listen on ‘all unassigned’ ip addresses, it will now pick up requests coming in on our local ip 127.0.0.1.
2. Navigate to your site and you will be taken to the sign in page.



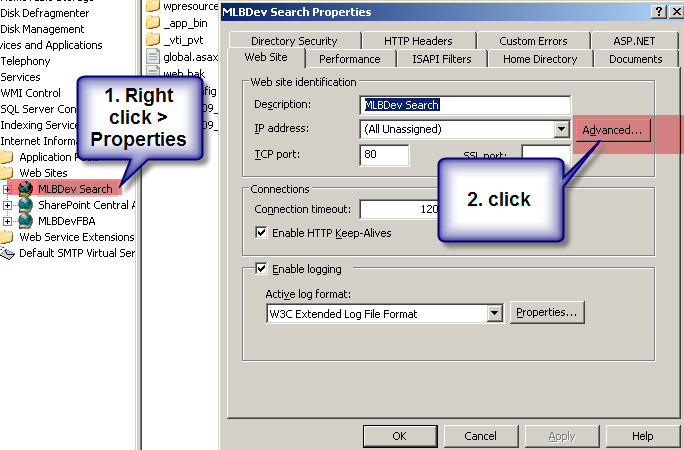
1. Log in (note the password in the client program in passw0rd# by default)



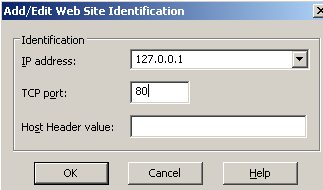
1. Hurray
2. You may choose while you are in here. If you don’t enable anonymous access, then you will want to go in and add a site collection administrator that is a Windows account so that you can test out search in the next section.

## Make your site searchable:

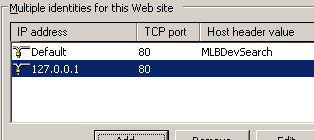
1. To make our site searchable, we’ll go back to the IIS manager and add an entry in our search web app that listens on port 80 of 127.0.0.1 and does not have a host header record.
2. Go back into your IIS Manager and open the properties for your search web app.



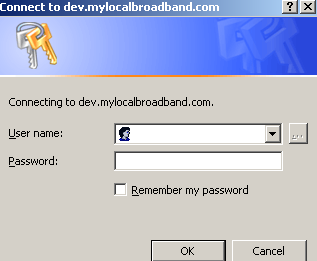
1. Then click the advanced button.
2. Click add and enter ip address 127.0.0.1 and port 80



1. Leave the host header value blank hand hit ok. You should have two records now that look like this.



1. At the very least, you’ll want to reset the SharePoint search service, do an IIS reset here and close all your browser windows. You may want to do a full server reboot.
2. To verify the windows authenticated web app is responding correctly.
   1. Reload your site (<http://dev.mylocalbroadband.com>)
   2. If you did not enable anonymous access, then you are immediately presented with a windows log in dialog box. Log in here and skip to step 5.
   3. If you enabled anonymous access, then after the site comes up, click the sign in link
   4. 
   5. You should then get a windows authentication prompt.

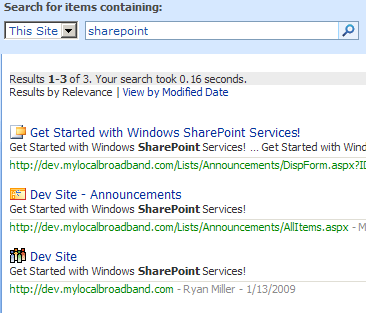


* 1. There is no need to log in, just cancel and then reload your site (or hit the back button).
  2. If you did not enable anonymous access, then you should already get the windows authentication prompt when the site is loaded. Log in here.

1. Give the site time to index. I usually allow about 30 minutes for this first time.
2. Try searching for SharePoint.



1. You should see a few returns, including at least the default announcement.



1. If you don’t get any results, check out: Search Troubleshooting below.

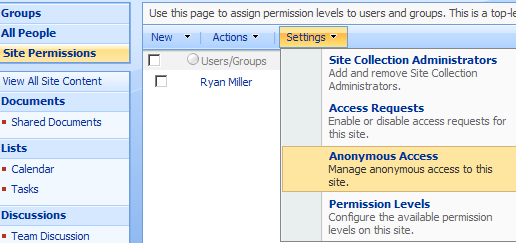
## Finalizing

That’s it. Any browser off this machine that hits your site will do so using our forms based authentication membership provider. Read through the appendix for information on making the auto sign in (remember me) work as well as anonymous access.

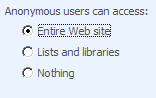
# Appendix:

## To enable anonymous access:

1. Go to the site permissions page (People and groups link, then site permissions link)



1. Choose Anonymous access from the settings tab.
2. Pick your poison and click OK

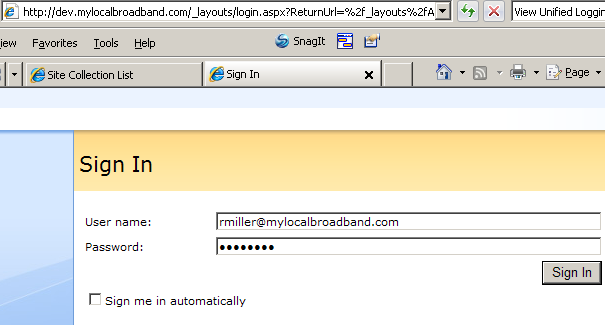


1. If you sign out now, you’ll still be able to browse the site, and there will be a sign in link at the top next to search.



## Making “Remember Me” Work

You’ll notice on the sign in page that there is a Sign me in automatically box.



If you try it, you’ll also notice that it doesn’t work correctly. It will remember you for 30 minutes and then you’ll need to sign in again.

**Hint: You’ll want to make this work if you want to use MS Office integration with your site.**

1. To fix this, open the web.config of your forms enabled web application (the one running on port 80)
2. Locate the authentication tag and add the below attributes to the forms tag.

<authentication mode="Forms">

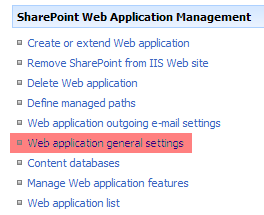
<forms loginUrl="/\_layouts/login.aspx" slidingExpiration="true" timeout="10080" />

</authentication>

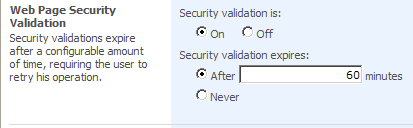
1. The timeout value is in minutes so 10080 = 7 days
2. The slidingExpiration = true means the authentication window will be reset after each authenticated hit on the website. So in this case with slidingExpiration = false, I would need to sign in every 7 days, but with slidingExpiration=true, I only need to sign in after a 7 day absence from the site.

### For clarity’s sake

Many admins new to forms based authentication think that you can set the automatic sign in window via central administration. If you go to the application tab’s web application general settings,



Midway down, you’ll see a section called Web Page Security Validation. Although this sounds like the automatic sign in setting, it is not.



Instead this setting controls the timing of how often the client’s browser is required to resend the user’s authentication. This doesn’t mean the user is required to type them in; this is something the browser handles for the user. There are good reasons to keep this setting turned on, but I’ll let you research that yourself (cop out, I know).

## Search Troubleshooting

First off, let me tell you that if you followed this demo and arrived here without search working, I feel your pain. As I said in the intro, this is my fourth time here myself and it’s a frustrating place to be. WSS search is a black box for which the logs will give you little to no insight. All you can do is shake the box and wait. That said, here’s how I’ve shaken the box to make it work.

* Restart the search service.
* Reboot the server. (of course)
* Use the client above to create another site. Dev1.mylocalbroadband.com for example.
* Try creating a new site, but use the other web app url, (if you used <http://MLBDevFBA> the first time, use <http://MLBDevSearch> this time.

These last two have given me the best results. I’m not sure why, but somehow they just kick start the indexer. Once search begins working, you should see it working on your original site too. You can then delete any of these extra site collections from Central Admin.