Working with Structured Data in Microsoft Office SharePoint Server 2007 (Part1): Configuring Single Sign On Service and Database

Applies to: Microsoft Office SharePoint Server 2007

Explore different options you have to work with structured data in a high volume while you need to perform complex queries and actions against such data ranging from authoring, approval and landing information on Web Part pages, all the way down to the physical storage. This article is part 1 of the blogs post series that I am planning to write on this topic. (13 printed pages)

Reza Alirezaei , Microsoft Office Server 2007 MVP
3/21/2009

* For comments please see http://blogs.devhorizon.com/reza/?p=832

Content:

Introduction: Data presentation is such a common requirement that it affects just about every layer of a platform on which you build your solution. Structured data must be stored somewhere, so deciding where to physically store your data is just as important as the techniques you leverage to interact with it. Typically, when it comes to working with structured data in SharePoint, you have three options:

> 1) Keep all your data in a backend system and query it real time. In case this is the first thing that comes to you mind, then you are certainly among those who believe that SharePoint is not meant to be used as a database management system.
>
> 2) Keep all your data in SharePoint. In another word, you use SharePoint as your main data repository which means no dependency on any other extra data sources. Less deployment headaches, less configuration and easier maintenance.
>
> 3) Use a hybrid approach. It is all about keeping the balance between great features lists and document libraries offer in SharePoint and what database engines can bring to the table. This approach may or may not require some extra work to keep both data structures in sync.

As you probably know, there are pros and cons associated with option number 1 and 2. Realistically speaking, neither of these options alone is the answer to all of your data integration woes in Microsoft Office SharePoint Server 2007. You like versioning, approval, bulk editing , rich UI and other good features that SharePoint lists offer but you are also concerned about the performance of your complex cross-list queries, CAML limitations (like 'join' , 'Select distinct') and optimized search over your content where BDC and search play very well together.

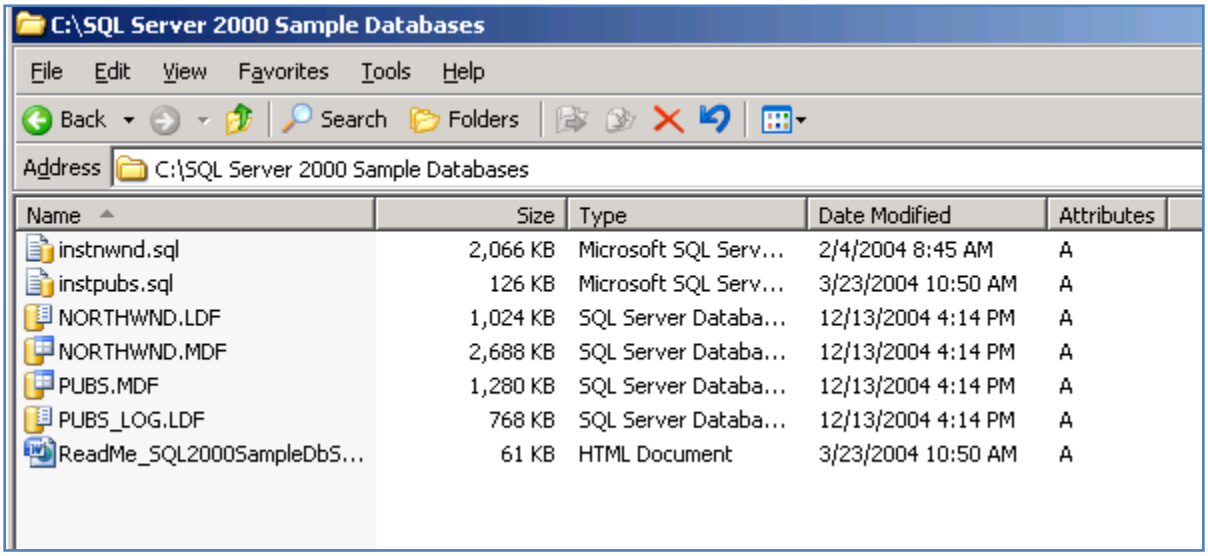
In reality, you need to provide a common metadata repository and a hybrid framework for accessing data stored in SharePoint and in external data sources utilizing all your options. These options include BDC, Data Form Web Part, BI capabilities of MOSS and eventually custom code to surface such information onto your SharePoint pages which works in both WSS 3.0 and MOSS 2007.

I will show you how you can surface information from your backend databases into your SharePoint sites , how to aggregate such information with the data structures already kept in SharePoint and many more fun stuff. I will leave the synchronization between data structures up to you to implement.

Creating the Northwind Database:

In this section, you will setup a connection to the Northwind sample database. As you probably know, Northwind is not the best database due to few new features in SQL Server Analysis Services 2005 and SQL Server Reporting Services 2005 (and that's why it is no longer part of SQL Server 2005 sample databases), but none of these features are important for our discussion here. That being said, in order to be consistent with my other blog posts and for the sake of simplicity, I decided to use Northwind database.

You can get the scripts for creating the Northwind sample database for use with SQL Server 2005 at http://www.microsoft.com/downloads/details.aspx?FamilyID=06616212-0356-46a0-8da2-eebc53a68034&displaylang=en. After extracting the files included in the download file, there should be a "SQL Server 2000 Sample Databases" folder which includes all the required files.

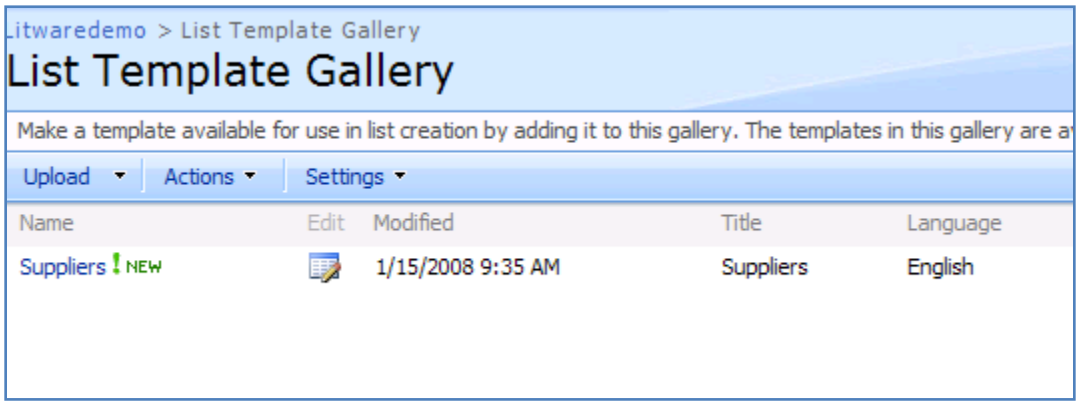


Go ahead and click on instnwnd.sql and click on "Execute" button in SQL Server management studio to create the Northwind database.

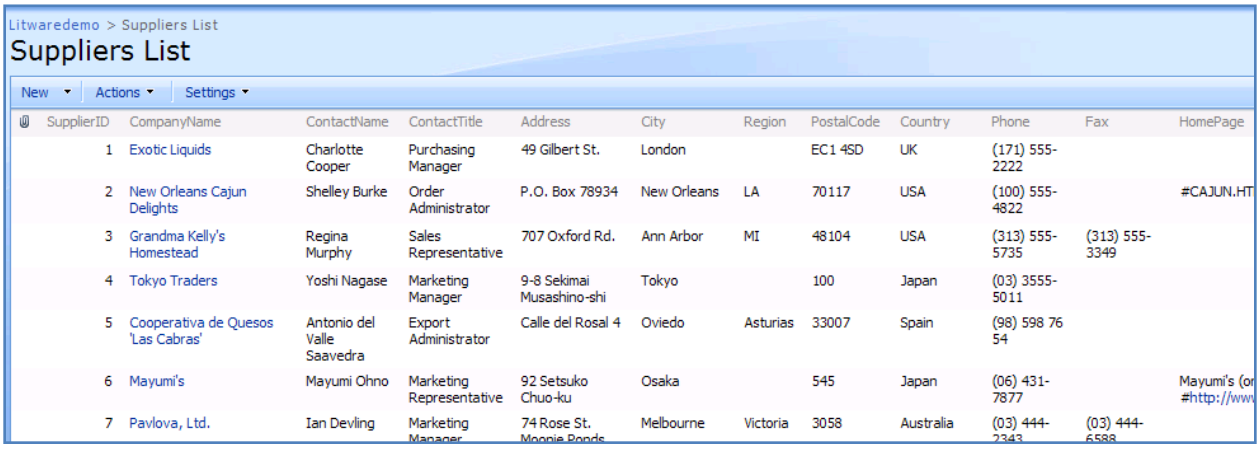
Creating the Suppliers List:

We will use a sample SharePoint List called "Suppliers" throughout these articles that can be downloaded at http://blogs.devhorizon.com/reza/wp-content/uploads/2008/03/Suppliers.rar. This list template is the exact representation of the Suppliers table in Northwind database and is meant to be used when aggregation of data between a SharePoint list and backend system is required.

First you need to upload the Suppliers list template to the List Template Gallery.



Next you need to create an instance of the suppliers list. Since the list template is created including the data, once the list is created, you will see that your list populated with information of 29 suppliers.



SupplierID	CompanyName	ContactName	ContactTitle	Address	City	Region	PostalCode	Country	Phone	Fax	HomePage
1	Exotic Liquids	Charlotte Cooper	Purchasing Manager	49 Gilbert St.	London		EC1 4SD	UK	(171) 555-2222		
2	New Orleans Cajun Delights	Shelley Burke	Order Administrator	P.O. Box 78934	New Orleans	LA	70117	USA	(100) 555-4822		#CAJUN.HT
3	Grandma Kelly's Homestead	Regina Murphy	Sales Representative	707 Oxford Rd.	Ann Arbor	MI	48104	USA	(313) 555-5735	(313) 555-3349	
4	Tokyo Traders	Yoshi Nagase	Marketing Manager	9-8 Sekimai Musashino-shi	Tokyo		100	Japan	(03) 3555-5011		
5	Cooperativa de Quesos 'Las Cabras'	Antonio del Valle Saavedra	Export Administrator	Calle del Rosal 4	Oviedo	Asturias	33007	Spain	(98) 598 76 54		
6	Mayumi's	Mayumi Ohno	Marketing Representative	92 Setsuko Chuo-ku	Osaka		545	Japan	(06) 431-7877		Mayumi's (or #http://www
7	Pavlova, Ltd.	Ian Devling	Marketing Manager	74 Rose St. Moonie Ponds	Melbourne	Victoria	3058	Australia	(03) 444-2343	(03) 444-6588	

Actual coding to make sure this list is sync with the our backend system is covered in great details in upcoming blogs posts.

Configuring SSO:

If your LOB data is located in a remote database server and if you also happen to be using NTLM as your authentication mechanism, you probably know that there is a catch when you're trying to access such data. The catch is double hop issue. Ouch!

Important
In a SharePoint environment, Windows credentials can only make one hop from the user's browser to the Web frond end server that the request is being processed. From that Web server to any backend system (second hop),Windows security token is no longer present ; therefore the call is rejected. This rejection surfaces in two forms. You are either prompted again for your credentials or your call dies silently due to the unauthorized second hop.

There are couple of ways to overcome this issue such as implementing Kerberos or Impersonating the end-user identity on the web server, but, thankfully, SSO functionality (shipped with MOSS 2007 Enterprise Edition) provides a secure alternative way for you.SSO gives you the ability to connect to the LOB system as a user specified in the SSO application definition. This will eliminate the second hop ; therefore you won't suffer from double hop issue anymore.

The out of the box Single Sign Service shipped with Microsoft Office SharePoint Server 2007 only works with Active Directory users and groups. This introduces two limitations:

1. You can't take advantage of the default SSO if you are not using a domain controller.
2. If the current user is not a Windows user, SSO doesn't work. As a result, FBA users can not be mapped to the SSO account which has enough permission to access the LOB system.

Fortunately, the SSO functionality in MOSS 2007, like many other features, follows the famous pluggable pattern which was first introduced in ASP.NET 2.0. This feature will give you the luxury of implementing your own SSO provider and plug it into the SharePoint runtime. Implementing an alternate SSO provider and replacing the default SSO provider in MOSS 2007 is covered in great details in future in this blog post series.

Important
Before configuring SSO, make sure that you install WSS 3.0 SP1 and MOSS 2007 SP1. There are couple of SSO issues that are fixed in MOSS 2007 SP1.

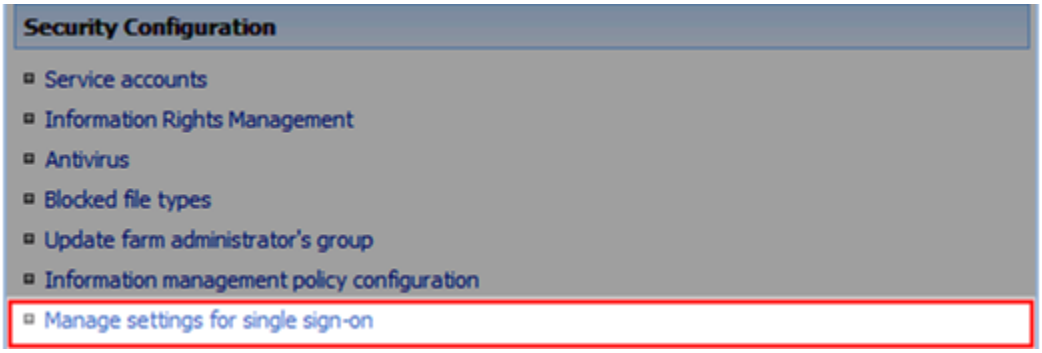
Configuring SSO is not as difficult as it sounds. You just need to follow five straightforward steps:

1. Run the Microsoft Single Sign-on Service on each Web front end and index server (For indexing the LOB data via BDC) across your farm.

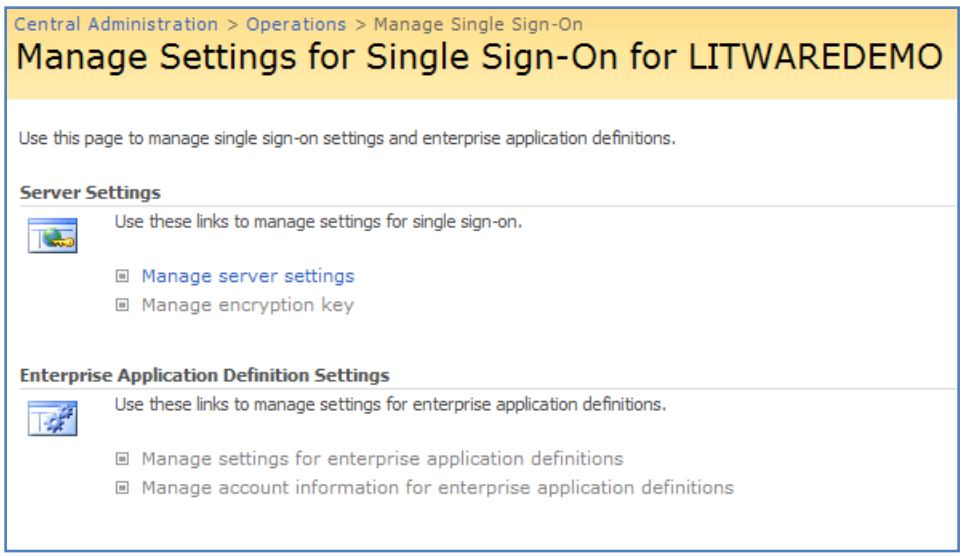
The first server on which you start SSOSrv (Executable for Microsoft Single Sign-on Service) is going to be your **encryption-key server**. The account that SSO service is configured to log on is very important. This is covered in great details at http://technet.microsoft.com/en-us/library/cc262932.aspx#Section1.

Important
Ensuring that SSO service is up and running , should be your first check when troubleshooting SSO.

2. Configure the required settings in central administration site --> Operations tab.



When you click on "Manage settings for single sign-on" link (Operations tab) for the first time, there is only one option available to you: Manager server settings. This totally makes sense as all the other settings are kind of dependant on the settings (SSO admin account, Enterprise App def account, SSO DB settings and Time out) you provide in the Manage server settings for SSO page.



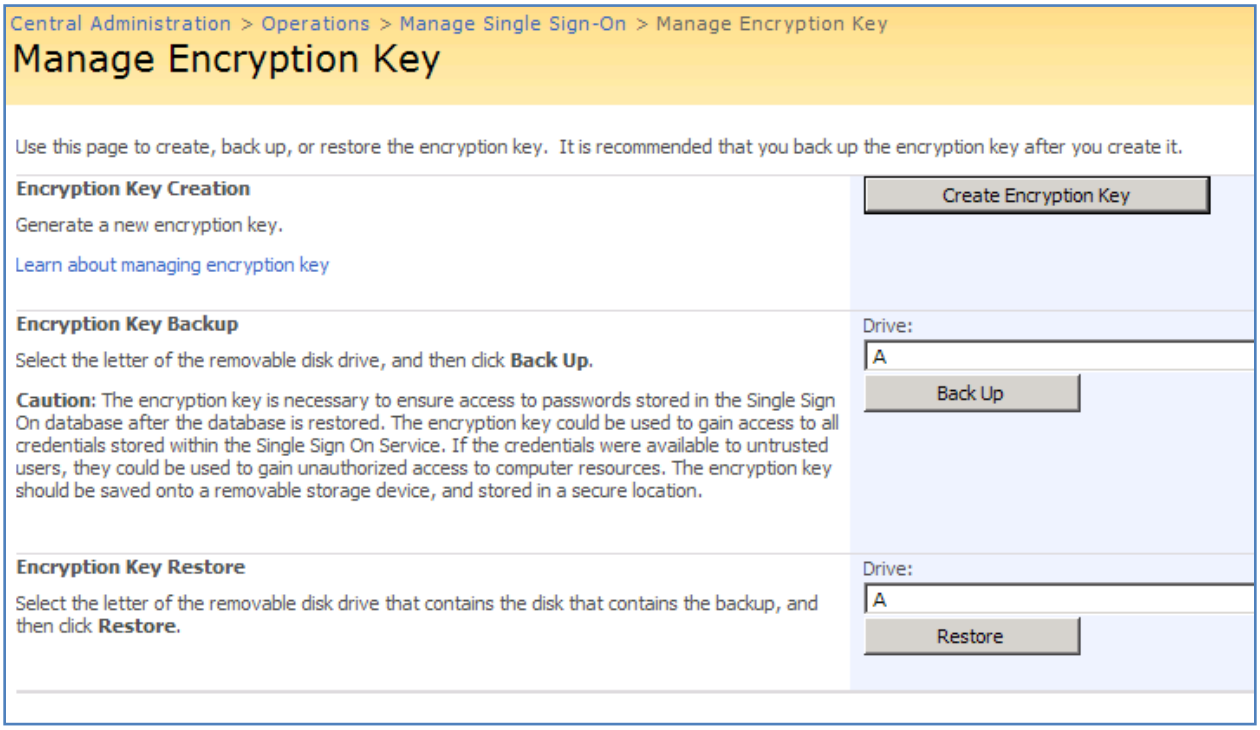
By clicking on "Manage Server settings" link above, you will be taken to the following page:

For more information on what you need to configure in this page and how to configure it, see http://technet.microsoft.com/en-us/library/cc262932.aspx#Section2

3. Create an encryption key. Use "Manage Encryption Key" page to create, back up, or restore the encryption key used for MOSS SSO. The fact that MOSS SSO uses a single master key to encrypt

all credentials can introduce some security vulnerabilities and limitations. Microsoft recommends that you create a new encryption key on a regular basis or when you suspect that account credentials have been compromised.

Last but not least, it is highly recommended that you back up the encryption key after you create it or each time you recreate it as mentioned above. For more information on Manage Encryption Key see http://technet.microsoft.com/en-us/library/cc262932.aspx#Section3.



4. Create an application definition .SSO's job is to create a mapping between a user (Litwareinc \BarbaraD), or group of users (Litwareinc\Traders) and the username and password needed to access a particular LOB system. It is worth mentioning that SSO application definition has nothing to do with BDC application definition. They are totally two different things.

   SSO app def can easily get deleted or modified by server administrators. Ensuring that SSO app def is still there and it matches with the app def which is used by client components (such as DFWP or UDCX connection file that an InfoPath form uses) is one of the important checks when troubleshooting SSO. There is also the possibility of password resets on one of the SSO account. In such cases, SSO app def must be reconfigured.

Important
LOB application (or LOB system) is a type of application that stores your business data, such as SQL Server, Oracle , SAP and etc.

In Create Enterprise Application Definition page , there are couple of fields that need to be highlighted here.

Account Type: Select **Group** to connect to the LOB system with the same account for all users. For example, all users in Litwareinc\Traders group will use Litwareinc\Traderuser account to connect to the LOB system.

Besides overcoming the double hop issue we discussed earlier in this post, there is another important reason to use SSO: Allowing domain users in a group , access your backend system using a single account. For example , imagine that all users in Litwareinc\Traders group must access Northwind database with read only permissions on Products, Suppliers and Categories tables. SSO lets you map Litwareinc\Traders group to Litwareinc\Traderuser account and give Litwareinc\Traderuser account read only permissions on those tables. This is a really cool feature in SSO!

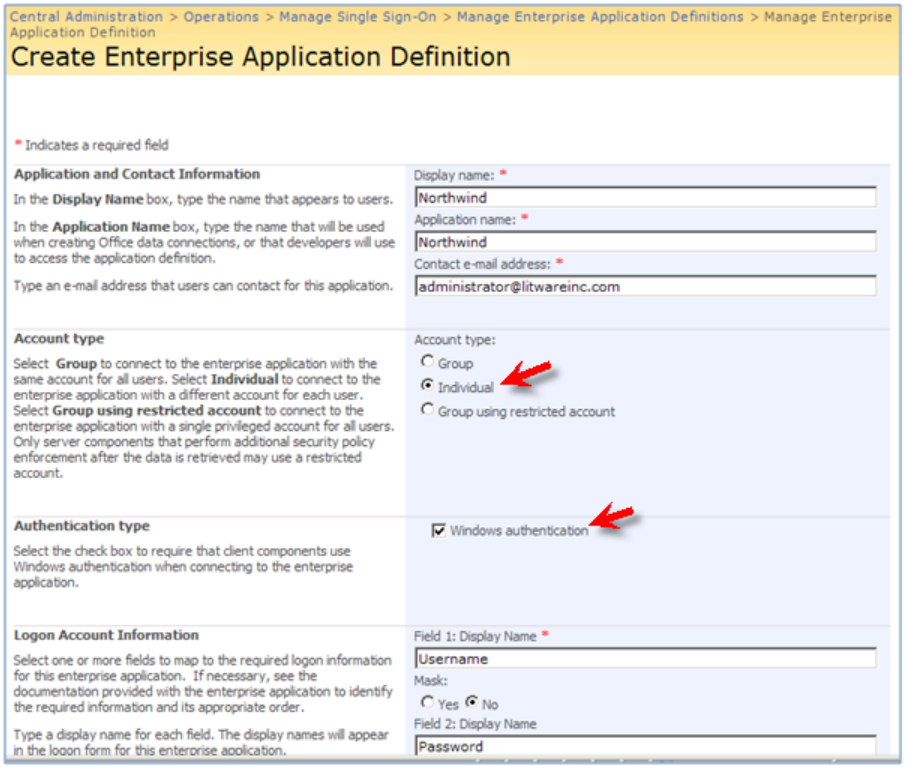
Select **Individual** to connect to the LOB system with a different account for each user. In another word , there is a one to one credential mapping when you choose Individual . For example, you can map the credential for Litwareinc \BarbaraD to Litwareinc\SsoNorthwind.

Select **Group using restricted account** to connect to the LOB system with a single privileged account for all users. Only server components that perform additional security policy enforcement after the data is retrieved may use a restricted account. For example , DFWP and Excel Services do not support such account type. BDC does!

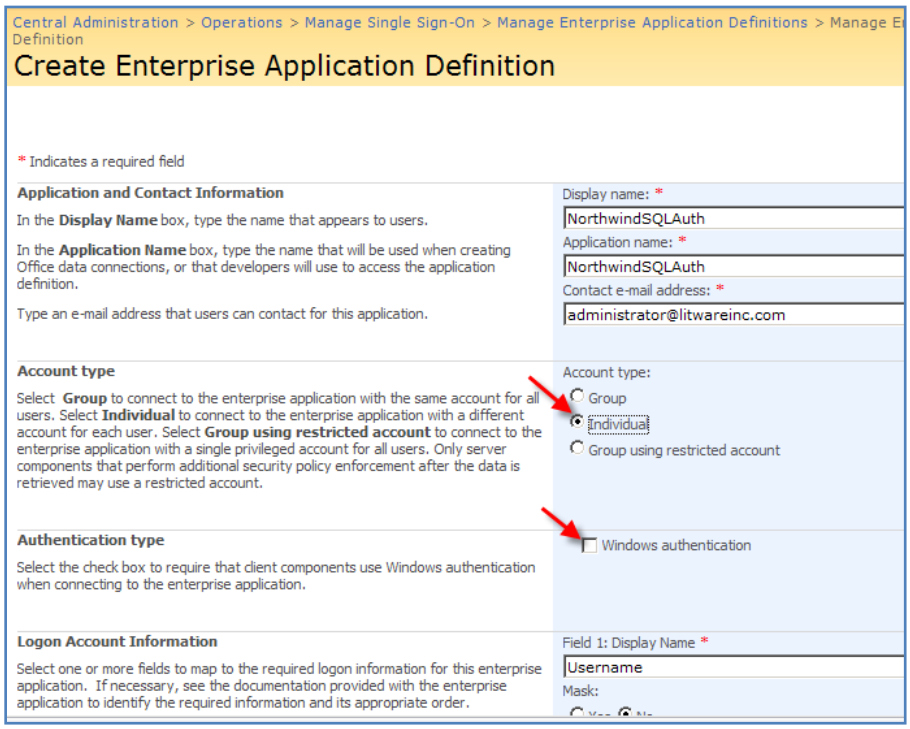
Authentication type: This is required if clients use Windows authentication when connecting to the LOB system, so it depends on your LOB system authentication type. For example, in an SQL server installation which supports mixed authentication (SQL and WIN), you need to leave this checkbox unchecked meaning both Windows and SQL Authentications are supported.

In this section, we will create three different types of SSO application definitions to provide credential mapping service to access Northwind database:

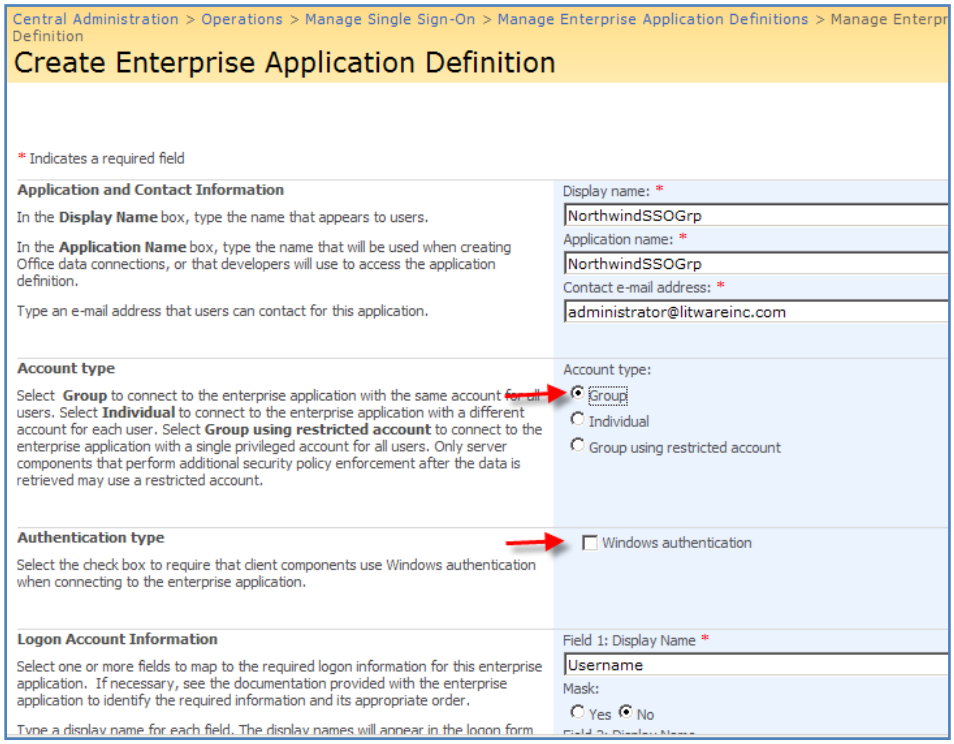
Northwind: Individual account type and with Windows Authentication



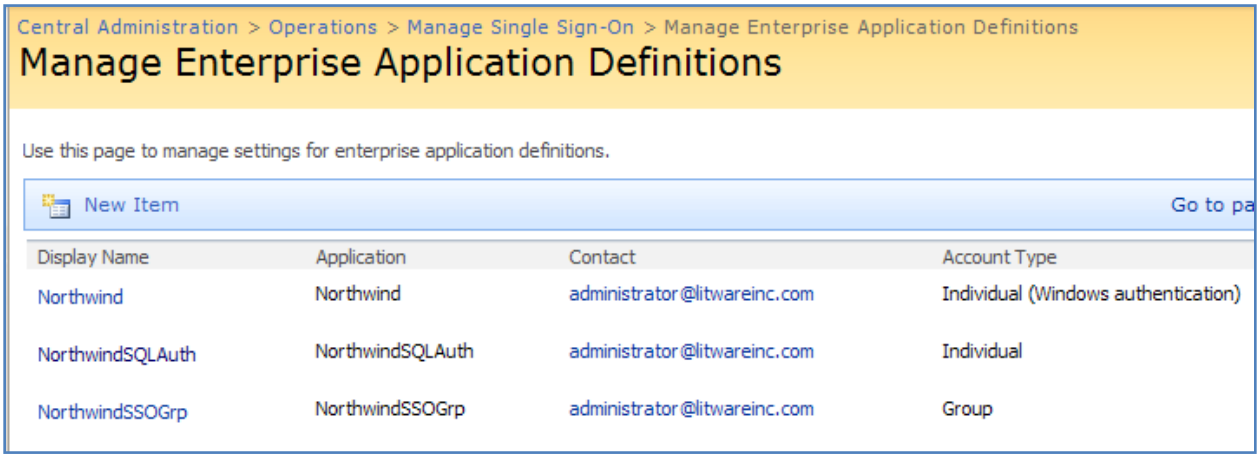
NothwindSQLAuth: Individual account type with SQL Authentication :



NorthwindSSOGrp : Group account type with Windows Authentication:



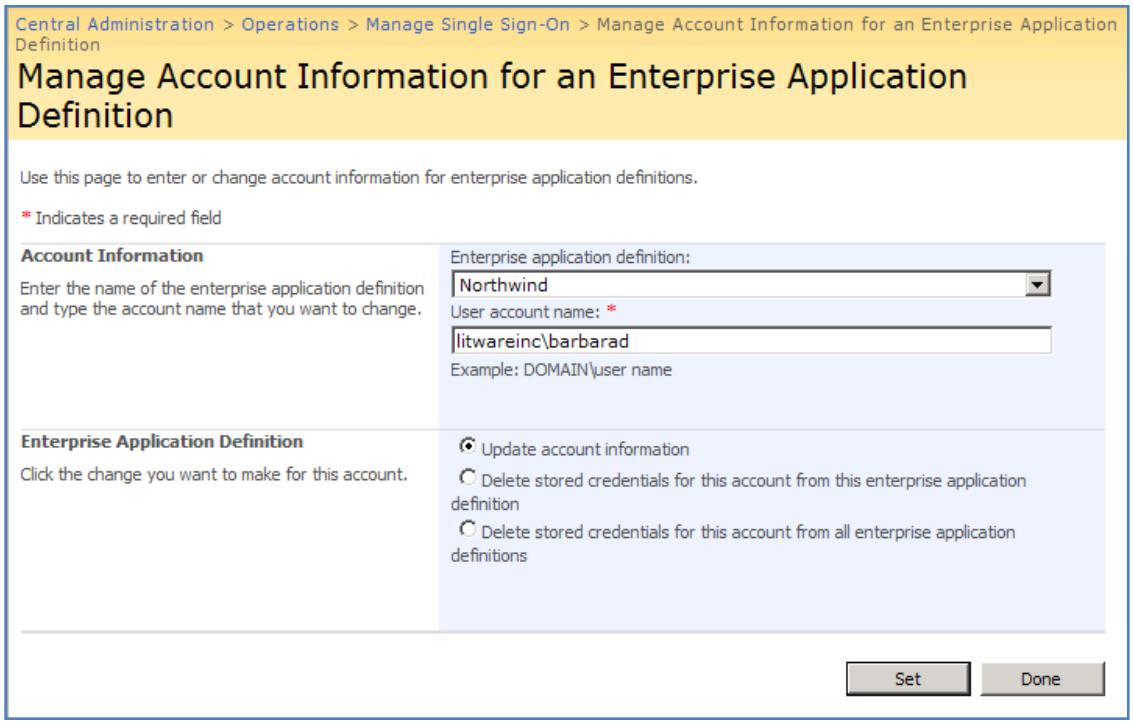
After creating all three application definitions, **Manage Enterprise Application Definitions** page should resemble the following:



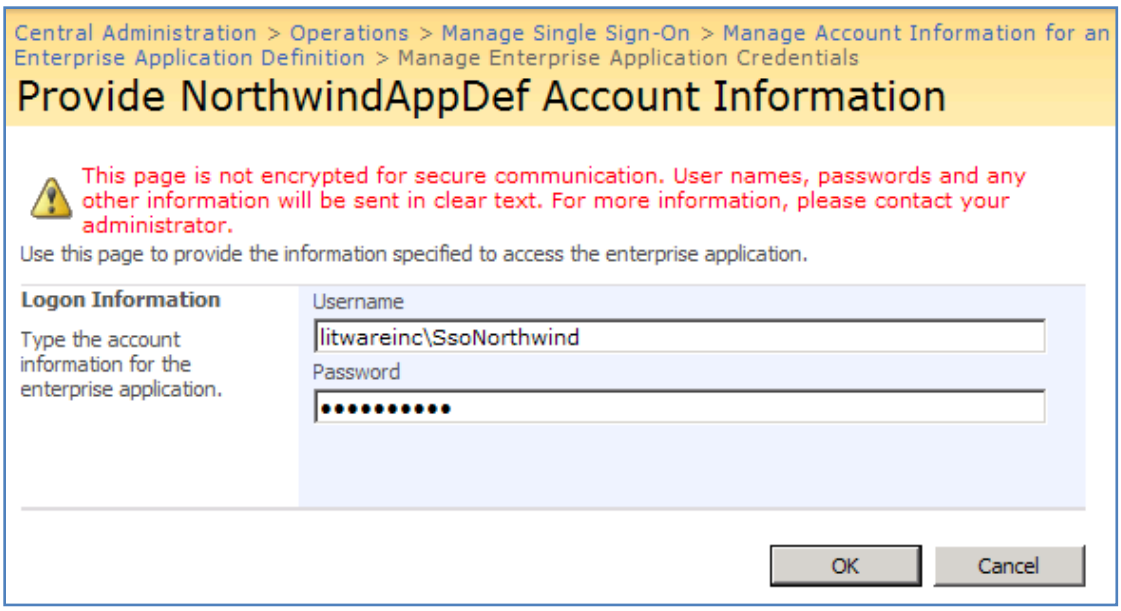
For more information on how to create a SSO application definition, see http://technet.microsoft.com/en-us/library/cc262932.aspx#Section4.

5. Configure the credential mapping for the application definition. This page is the heart of your SSO settings , where the actual magic (credential mappings) takes place. In total , there are two forms that you need to go through to create the credential mappings :

A) In this form, you specify your app def , the account (individual or group based on what you specified in step 4) and the action. For more information about the actions that you can take in this form , see http://technet.microsoft.com/en-us/library/cc262932.aspx#Section5. For example if you specified Litwareinc\Traders group as your SSO account above, you type in the group name. Since I am using Individual account type, I just used litwareinc\barbarad user account.



B) When you click on Set button in the last form, you will be taken to another form (below) where you provider the credentials for the account that is meant to be used to access the LOB system (in our case Northwind database hosted in SQL Server 2008). Click ok and you're done!



With our SSO service properly configured , we can now conclude this article that outlines the required preparation steps . Let's move on to Working with Structured Data in Microsoft Office SharePoint Server 2007 Part 2.

Additional Resources

- http://technet.microsoft.com/en-us/library/cc262932.aspx
- http://www.thorprojects.com/blog/archive/2008/08/02/moss-single-sign-on-setup-step-by-step.aspx