



SSO BDC IS EASY!

BY BRETT LONSDALE, MCTS, MCSO.NET, MCT

LIGHTNING TOOLS

WWW.LIGHTNINGTOOLS.COM

BRETT@LIGHTNINGTOOLS.COM

PRE-REQUISITES

This Whitepaper is written assuming that you have a good understanding of what The Business Data Catalog is, and you have a good general understanding of SharePoint 2007. If you are new to the Business Data Catalog, then please see the 'Introduction to BDC' whitepaper which is available for free download from <http://www.lightningtools.com> prior to reading this whitepaper.

INTRODUCTION

First of all, let's clarify why we need to use SSO with BDC. Usually Single Sign-On (SSO) is used for Credential Mapping so that you are not prompted again for your username and password when accessing data from a backend system. Meaning that, if you have already logged onto SharePoint, and you are a member of a domain group, your credentials will be mapped to a user account that has permissions to access the database, and SharePoint doesn't need to challenge you again for your credentials.

Where BDC is concerned that hurdle can be overcome in other ways as well as using SSO. BDC can use different Authentication Mechanisms such as Passthrough or RevertToSelf. If using RevertToSelf you are asking the Application Pool ID to access the database for you, so that each user doesn't need a specific login account locally at the database. Using PassThrough means that the users' credentials are passed through to the database and the user will require a login account and permissions to the database.

Typically in a real world SharePoint environment your SQL/Oracle database (aka Line of Business Data) will reside on a remote server to the SharePoint Web Front End Server (WFE). When we describe Line of Business data (LOB) we are referring to: Microsoft Navision, Microsoft Great Plains, Oracle Financials, or any type of database that stores Business data such as Customers, Suppliers, Orders etc..

If your LOB database is remote, and you also happen to be using Network LAN Manager (NTLM) as an Authentication mechanism for Integrated Security you will suffer from what is known as the Double Hop Issue. If you haven't come across the double hop issue by now, you will do soon if you try accessing remote data from SharePoint whilst using NTLM. NTLM can only make one hop. One hop is from Internet Explorer (IE) to Internet Information Services (IIS). Unfortunately credentials need to be passed from IE to IIS to your database server (Two Hops). SSO is able to connect to the data source as a user specified in the SSO Application Definition and temporarily logs in as that user, meaning only one hop is required to access the data source.

The Double Hop issue is just one reason to use SSO. Another reason is that you want to make use of your Active Directory (AD) groups when accessing data. This means that you can provide access to the data from a domain group such as 'domainname\sales' or 'domainname\domain users' to the database using a specific account.

Of course the Credential Mapping is still very useful as I don't need a login account at the database. If I am a member of a group such as 'Domain Users' then 'Domain Users' can be configured to always connect to the database as DomainName\Administrator or another account that has Read permissions to the database.

In this WhitePaper we are going to learn how to configure SSO, as well as discussing best practices and reasons for using SSO. We will then learn how to configure your Application Definition File for BDC so that it takes advantage of SSO when connecting to your remote database.

The setup used to write this White Paper is:

- Microsoft Vista Ultimate Host Operating System
 - Microsoft Virtual PC 2007
- Microsoft Windows Server 2003 Service Pack 2 Stand Alone
 - Microsoft SQL Enterprise Edition 2005
 - ASP.NET
 - IIS 6.0
 - Microsoft Office SharePoint Server 2007 Enterprise Edition
 - Adventure Works Database
 - Microsoft Office Ultimate 2007
 - Microsoft Visual Studio 2005 Professional Edition
 - Oracle 10g

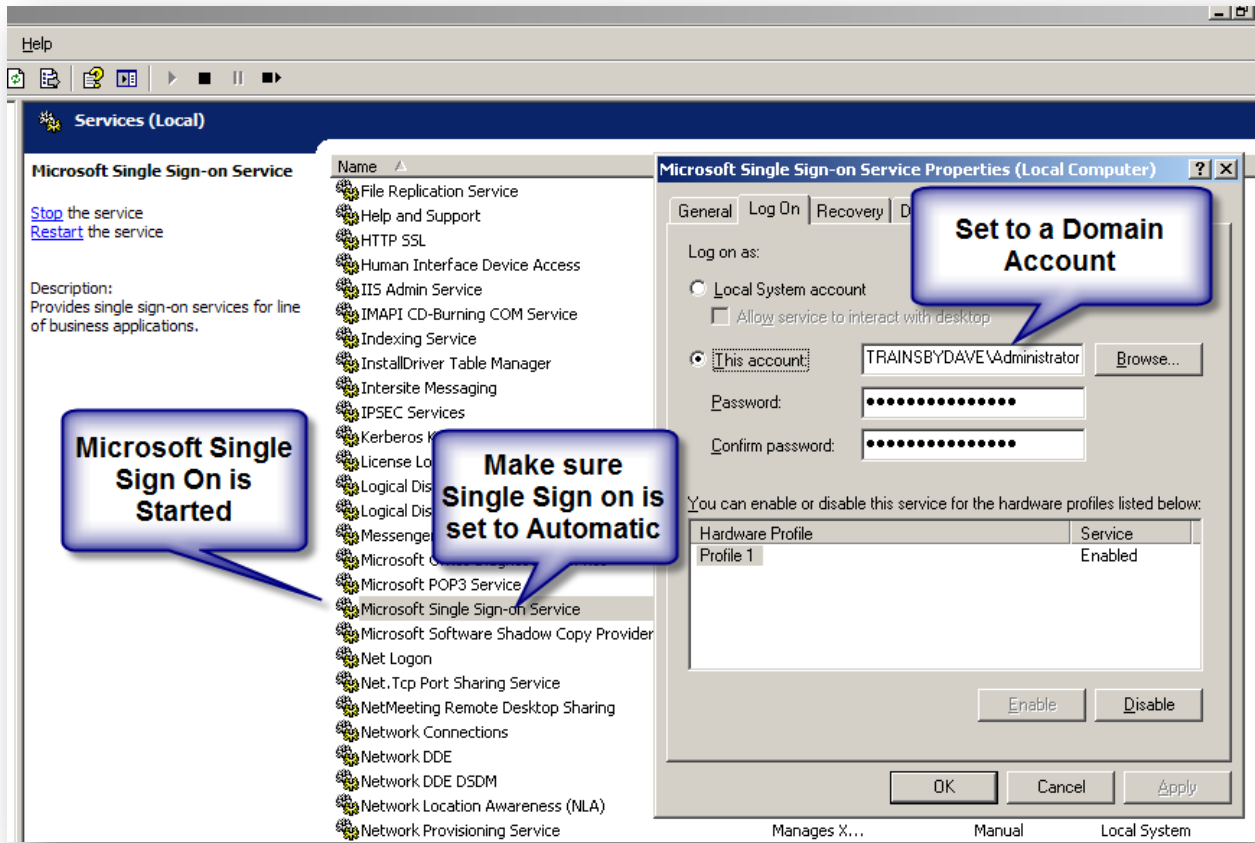
CONFIGURING SSO

Configuring SSO is probably the most straight forward part of using SSO with BDC and is configured in five easy steps:

1. Firstly you need to ensure that the Microsoft Single Sign-On Service is running on every WFE. If you intend to use BDC Searching, you will also need to make sure that the Microsoft Single Sign on Service is running on the index server as well. You can learn how to configure BDC search from my article listed in the December 2007 issue of [SharePoint Beagle](#)
2. Secondly, we can navigate to SharePoint Central Administration where the rest of the configuration of SSO will take place. We will need to configure the Settings for SSO which includes specifying the Single Sign-On Administrative Account, The Enterprise Application Definition Administrative Account and the Timeout settings for Single Sign on tickets.
3. Create your Encryption key that will be used to encrypt the credentials that are stored in the SSO database. Make sure the Encryption key is backed up.
4. Create an Application Definition. This is not the same as an Application Definition File for BDC. Application Definition in SSO refers to the Back End Database that you will be connecting to.
5. Configure the Credential Mapping for the Enterprise Application Definition.

STARTING THE SINGLE SIGN ON SERVICE


1. On each SharePoint Web Front End Server, Index Server, or Excel Services Server choose **Start, Administrative Tools, Services**.
2. Right click on **Microsoft Single Sign On Service**, and choose **properties**
3. Under the **General Tab**, in the **Startup Type** field, change the start up type to **Automatic**
4. Click the **Log On** tab, and change the account to be:
 - a. A Domain User Account (Not Group)
 - b. A MOSS Farm Account
 - c. A Member of the Local Administrators group on the Encryption Key Server
 - d. Must have DB_Creator & Security Administrators roles on the SQL Server for SharePoint
 - e. Must be the Single Sign On Administrative Account or a member of the SSO Admin Group. (See next section of this whitepaper on how to configure the SSO Admin account).
5. Click **OK**.



MANAGE THE SETTINGS FOR SINGLE SIGN ON

1. Navigate to **SharePoint Central Administration** by choosing **Start, Administrative Tools, SharePoint 3.0 Central Administration**
2. Click the **Operations Tab**
3. In the Security Configuration Section Click '**Manage Settings for Single Sign On**'

Central Administration Welcome TRAINSBYDAV

 **Central Administration**

Home **Operations** Application Management

Central Administration > Operations

Operations

This page contains links to pages that help you manage your server or server farm, such as changing the server farm to running on each server, and changing settings that affect multiple servers or applications.

Server Farm Configuration Not Complete

See [administrator task list](#) for more information


View All Site Content

Central Administration

- Operations
- Application Management

Shared Services Administration

- SSP01

 **Recycle Bin**

Topology and Services

- Servers in farm
- Services on server
- Outgoing e-mail settings
- Incoming e-mail settings
- Approve/reject distribution groups

Security Configuration

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group
- Information management policy configuration
- Manage settings for single sign-on

Global Configuration

- Timer job status
- Timer job definitions
- Master site directory settings
- Site directory links scan
- Alternate access mappings
- Quiesce farm
- Manage farm features
- Solution management

Backup and Restore

- Perform a backup
- Backup and restore history
- Restore from backup
- Backup and restore job status


Logging and Reporting

Data Configuration

Manage Settings for Single Sign On

4. Click **Manage Server Settings** from the Server Settings section

Central Administration Welcome TRAI

 **Central Administration**


Home **Operations** Application Management

Central Administration > Operations > Manage Single Sign-On

Manage Settings for Single Sign-On for MOSS01


Use this page to manage single sign-on settings and enterprise application definitions.

Server Settings

 Use these links to manage settings for single sign-on.

- [Manage server settings](#)
- [Manage encryption key](#)

Enterprise Application Definition Settings

 Use these links to manage settings for enterprise application definitions.

- [Manage settings for enterprise application definitions](#)
- [Manage account information for enterprise application definitions](#)

Server Farm Configuration Not Complete

See [administrator task list](#) for more information


[View All Site Content](#)

Central Administration

- [Operations](#)
- [Application Management](#)

Shared Services Administration

- [SSP01](#)

 [Recycle Bin](#)

5. Set the **Single Sign-On Administrative Account** which will be able to create, Edit, and delete Application Definitions for SSO. This account must be an Individual Domain User or a Global Domain Group Account. It must also be the same as the Configuration Account if you have specified a User Account or if you specify a Global Group then it must be the same group that contains the Configuration Account. Set this in the format: DomainName\AccountName.
6. Set the **Enterprise Application Definition Administrator Account**. The User/Group here will be able to configure the Credential Mapping for each Application Definition. Configure this in the format DomainName\AccountName.
7. Set the **SQL Server Database name** including the instance name if one exists e.g. MOSS01\OfficeServer or MOSS01
8. Set or leave the **Ticket Time Out**. (SSO issues a ticket when a request is made by an authorized user. The ticket includes the encrypted username and password of the authenticated user and the timeout. The timeout is set to 2 minutes by default which is recommended.)
9. Finally set the **Number of days** to keep Audit records for. The default is 10 days.

<p>Single Sign-On Administrator Account</p> <p>In the Account name box, type the name of the group or user account that can set up and manage the single sign-on service. This account must be a member of the same domain to which the single sign-on service account belongs.</p> <p>Learn about managing Single Sign-On</p>	<p>Account name: *</p> <input type="text" value="TRAINSBYDAVE\Administrator"/> <p>Example: DOMAIN\group name or DOMAIN\user name</p>
<p>Enterprise Application Definition Administrator Account</p> <p>In the Account name box, type the name of the group or user account that can set up and manage enterprise application definitions. This account must be a member of the same domain to which the single sign-on service account belongs.</p>	<p>Account name: *</p> <input type="text" value="TRAINSBYDAVE\Administrator"/> <p>Example: DOMAIN\group name or DOMAIN\user name</p>
<p>Database Settings</p> <p>In the Server name box, type the name of the database server that stores the settings and account information for single sign-on.</p> <p>In the Database name box, type the name of the single sign-on database.</p>	<p>Server name: *</p> <input type="text" value="MOSS01"/> <p>Examples: computer name or computer name\SQL Server instance</p> <p>Database name: *</p> <input type="text" value="SSO"/>
<p>Time Out Settings</p> <p>In the Ticket time out box, type the number of minutes to wait before allowing a ticket to time out.</p> <p>In the Delete audit log records older than box, type the number of days to hold records in the audit log before deleting.</p>	<p>Ticket time out (in minutes): *</p> <input type="text" value="2"/> <p>Example: 2</p> <p>Delete audit log records older than (in days): *</p> <input type="text" value="10"/> <p>Example: 10</p>

MANAGE THE ENCRYPTION KEY

You can only have one Encryption Key Server where the Encryption key is generated. This Server is the one where you first enabled the Single Sign-On Service in step 1. The Encryption key is used to encrypt the credentials stored in the SSO database for each user. Make sure that you have a backup of the Encryption key, and recreate it periodically. The recommended period is 90 days.

1. From the **Manage Single Sign-On** page click **Manage Encryption Key**
2. Click **Create Encryption Key**.
3. Ensure that the Check Box is selected to **Re-encrypt all credentials** using the new encryption key.
4. Optionally Backup the Encryption Key.

Manage Encryption Key

Use this page to create, back up, or restore the encryption key. It is recommended that you back up the encryption key after you create it.

Encryption Key Creation

Generate a new encryption key.

[Learn about managing encryption key](#)

Create Encryption Key

Encryption Key Backup

Select the letter of the removable disk drive, and then click **Back Up**.

Caution: The encryption key is necessary to ensure access to passwords stored in the Single Sign On database after the database is restored. The encryption key could be used to gain access to all credentials stored within the Single Sign On Service. If the credentials were available to untrusted users, they could be used to gain unauthorized access to computer resources. The encryption key should be saved onto a removable storage device, and stored in a secure location.

Drive:

A

Back Up

Encryption Key Restore

Select the letter of the removable disk drive that contains the disk that contains the backup, and then click **Restore**.

Drive:

A

Restore

CREATING AN APPLICATION DEFINITION

Each Database you want to set SSO up for is referred to as an Application Definition. The Application Definition is the mapping of credentials for each user or group that is able to authenticate with the database. To configure the Application Definition:

1. From the **Manage Single Sign-On page** choose **Manage Settings for Enterprise Application Definitions** from the Enterprise Application Definition Settings section.
2. Choose **New Item** to create a new Application Definition
3. Type a **Display Name** for the Application Definition e.g. Adventure Works. This will display in the places such as the Data Form web Part.
4. Type the **Application Name** e.g. AdventureWorks. This is what you will use to connect to the Data Source using your BDC Application Definition File (ADF) or also in the Data Form Web Part Properties.
5. Type a **contact email address** – usually the SSO Administrator.
6. The **Account Type field** depends on the results that you require. You can select from **Group, Individual, or Group Using Restricted Account**.

Account type

Select **Group** to connect to the enterprise application with the same account for all users. Select **Individual** to connect to the enterprise application with a different account for each user. Select **Group using restricted account** to connect to the enterprise application 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.

Account type:

- Group
- Individual
- Group using restricted account

- a. **Group** – Select Group if you want a Domain Group to access the database using a particular account. E.g. If you want your Sales department to access the database as one user then choose this option. You will then be able to map the credentials for that group such as: DOMAINNAME\Sales -> DOMAINNAME\SalesUser. The Sales User will have the permissions on the database tables that are required by sales people. E.g. The DOMAINNAME\Sales group may have Read Permissions on the Customers, Orders, Order Details tables but no permissions on the Suppliers table.
 - b. **Individual** – Select individual if you want to map the credentials for a User Account to another user Account. For example: DOMAINNAME\Brett -> DOMAINNAME\Administrator. When using the Data Form Web Part, If the user doesn't have stored credentials when trying to access the database, they will be prompted the first time, and then Credentials will be stored for them so that they are not prompted again.
 - c. **Group using restricted account** – Choose this option if you are going to use a group such as DOMAINNAME\Domain Users so that all users will be able to access the database via SSO. The group name will still access the database with a specific user account. This option uses a different API to the other two options to access the database. It is worth noting that SharePoint Designer and Excel Services do not support this option. Use this option when using BDC that applies further trimming of security so that a security breach doesn't occur using a privileged account.
7. Set the **Authentication Type** depending on your SQL Server Authentication. If you are using Mixed Mode in SQL then you will need to have the Authentication Type check box cleared. If you are using Windows Authentication, then this option will need to be checked. The Same Applies to Oracle, check this if you are using Windows Authentication on your Oracle Server. Note that the Account that accesses the database will be authenticated using Windows Authentication, and not the User that is logged into SharePoint.
 8. **Logon Account Information** – provides you with the ability to setup all the required information to access the data source. E.g. If accessing a SQL Server, you may only need to prompt for: Username & Password. So you can proceed with the default settings for Field 1 & Field 2. However, you may also want to prompt for additional information especially if you have created your own Web Part that requires information to access the data source. E.g. If you are using Oracle you may set Field 1 to Oracle User Name, Field 2 to Oracle Password, and Field 3 to Oracle Database Name. If you are using a Group account rather than an individual account, then you can set the credentials using the next step: Manage

Account Information for Enterprise Application Definitions. This has to be performed by a SSO Administrator.

9. Click **Ok**

Application and Contact Information In the Display Name box, type the name that appears to users. In the Application Name box, type the name that will be used when creating Office data connections, or that developers will use to access the application definition. Type an e-mail address that users can contact for this application.	Display name: * <input type="text" value="AdventureWorks"/> Application name: * <input type="text" value="AdventureWorks"/> Contact e-mail address: * <input type="text" value="a@b.com"/>
Account type Select Group to connect to the enterprise application with the same account for all users. Select Individual to connect to the enterprise application with a different account for each user. Select Group using restricted account to connect to the enterprise application 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.	Account type: <input checked="" type="radio"/> Group <input type="radio"/> Individual <input type="radio"/> Group using restricted account
Authentication type Select the check box to require that client components use Windows authentication when connecting to the enterprise application.	<input type="checkbox"/> Windows authentication
Logon Account Information Select one or more fields to map to the required logon information for this enterprise application. If necessary, see the documentation provided with the enterprise application to identify the required information and its appropriate order. Type a display name for each field. The display names will appear in the logon form for this enterprise application. Clicking Yes for Mask will hide the text typed by the user. This helps ensure that sensitive information such as a password is not displayed.	Field 1: Display Name * <input type="text" value="Username"/> Mask: <input type="radio"/> Yes <input checked="" type="radio"/> No Field 2: Display Name <input type="text" value="Password"/> Mask: <input checked="" type="radio"/> Yes <input type="radio"/> No Field 3: Display Name

MANAGE ACCOUNT INFORMATION FOR AN ENTERPRISE APPLICATION DEFINITION

You perform this next step if you are using one of the two Group options. You can also configure individual credential mapping using this option alternatively users can be prompted for credentials when using the Data Form Web Part instead of BDC. Since we are using BDC and more than likely Group credentials we will go through the steps.

1. From the **Manage Single Sign-On** page, choose **Manage Account Information** for an Enterprise Application Definition.
2. Select the **Required Enterprise Application Definition** from Enterprise Application Definition field.
3. Enter the **Group Account Name** for the Group you intend to set the credentials for. In this example I am using TRAINSBYDAVE\Sales.

4. Click the **Set** button

Central Administration > Operations > Manage Single Sign-On > Manage Account Information for an Enterprise Application Definition

Manage Account Information for an Enterprise Application Definition

Use this page to enter or change account information for enterprise application definitions.

* Indicates a required field

Account Information
Enter the name of the enterprise application definition and type the account name that you want to change.

Enterprise application definition:
AdventureWorks

Group account name: *
TRAINSBYDAVE\sales
Example: DOMAIN\group name

Enterprise Application Definition
Click the change you want to make for this account.

Update account information
 Delete stored credentials for this account from this enterprise application definition
 Delete stored credentials for this account from all enterprise application definitions

Set Done

5. You will be taken to a page where you can provide the username and password for the account that will access the data source.

Central Administration > Operations > Manage Single Sign-On > Manage Account Information for an Enterprise Application Definition > Manage Enterprise Application Credentials

Provide AdventureWorks Account Information

This page is not encrypted for secure communication. User names, passwords and any other information will be sent in clear text. For more information, please contact your administrator.

Use this page to provide the information specified to access the enterprise application.

Logon Information
Type the account information for the enterprise application.

Username
TRAINSBYDAVE\Administrator

Password

OK Cancel

6. Click **OK**.

CREATING THE BDC APPLICATION DEFINITION FILE

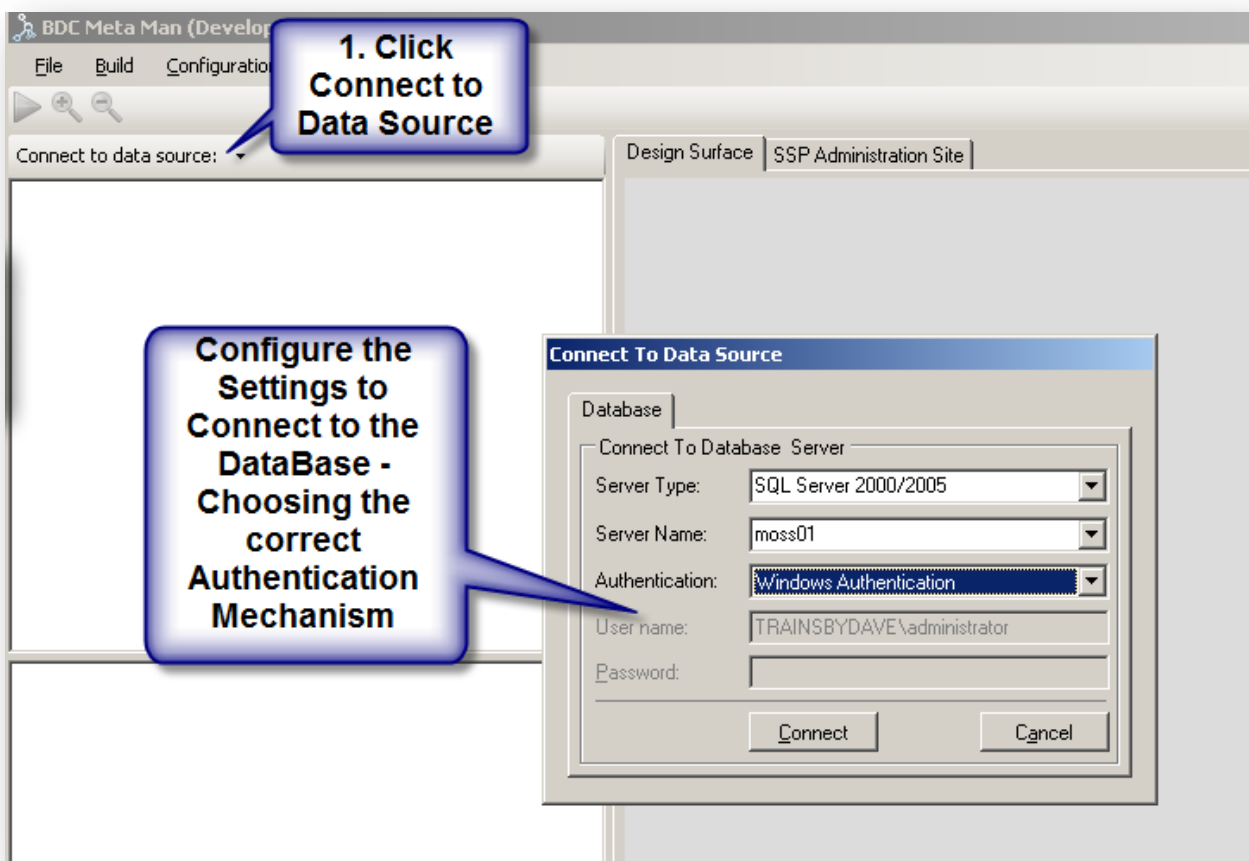
Currently BDC Meta Man doesn't provide you with the option of configuring SSO in your Application Definition. However, you can use BDC Meta Man or Microsoft's BDC Definition Editor to create your

Application Definition file, and then make a couple of changes to the file prior to importing it into SharePoint Farm.

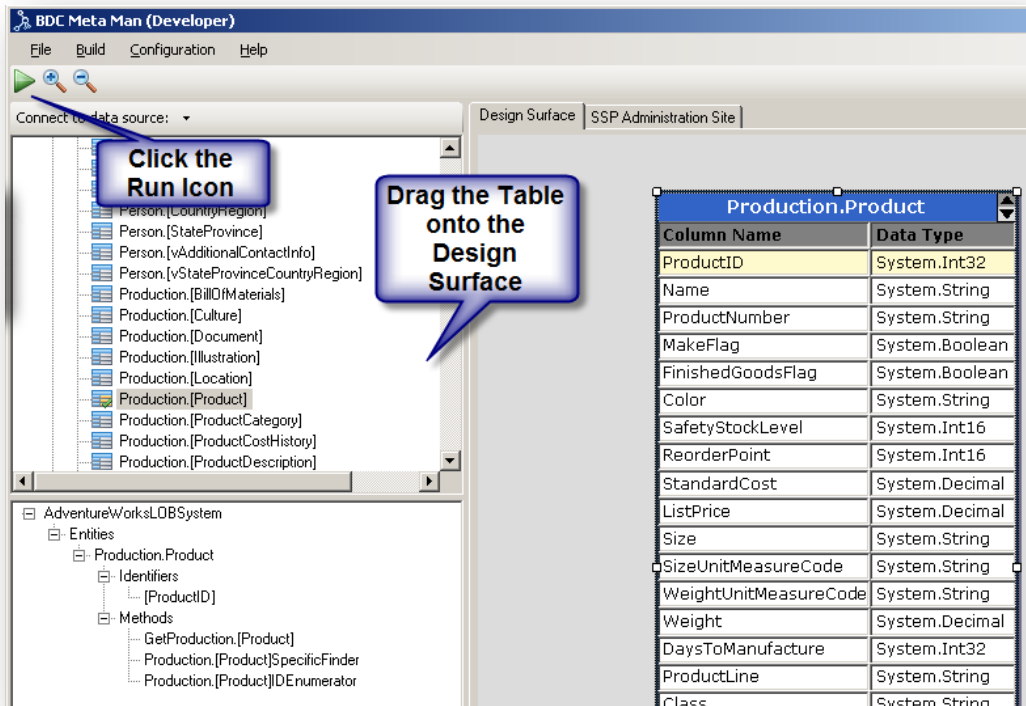
In my examples I used BDC Meta Man to create an Application Definition File for Adventure Works in SQL and Employees in Oracle.

Follow these steps to configure the connection to SQL using the 'Free' Developer edition of BDC Meta Man:

1. Launch **BDC Meta Man** (Downloadable from www.bdcmetaman.com)
2. Click '**Connect to data source**'
3. Configure the properties of the connection.



4. **Expand** your database from the Database explorer window on the left hand side of the form.
5. **Drag** the Table/Tables onto the design surface that you want to connect to.
6. There are other properties that you can configure, but I am now going to generate the Application Definition File by choosing Configuration, Settings, and then setting the filename.
7. Click the green **Run** Icon to generate the file.



8. **Edit the generated Application Definition** file using an editor such as Visual Studio.NET.
9. Change the **AuthenticationMode** Property to '**WindowsCredentials**'
 - a. **PassThrough** – is used when the Database Server is local to the SharePoint WFE and you want to access the database using the users authenticated credentials.
 - b. **WindowsCredentials** – Used in conjunction with SSO and forces BDC to access use the credentials from the Single Sign-On system.
 - c. **RevertToSelf** – Used to overcome the double hop issue and accesses the Database Server using the Application Pool ID
10. **Add the following Property** to specify which SSO Application Definition to use:

```
<Property Name="SsoApplicationId"
Type="System.String">AdventureWorks</Property>
```

11. Add the following Property to set the SSO Provider Class:

```
<Property Name="SsoProviderImplementation"
Type="System.String">Microsoft.SharePoint.Portal.SingleSignon.SpsSsoProvider, Microsoft.SharePoint.Portal.SingleSignon, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c</Property>
```

12. Your finished ADF should resemble the following:
13. **Save** the Changes.

```

<LobSystemInstances>
  <LobSystemInstance Name="AdventureWorksInstance">
    <Properties>
      <Property Name="DatabaseAccessProvider" Type="System.String">SqlServer</Property>
      <Property Name="AuthenticationMode" Type="System.String">WindowsCredentials</Property>
      <Property Name="RdbConnection Data Source" Type="System.String">moos01</Property>
      <Property Name="RdbConnection Initial Catalog" Type="System.String">AdventureWorks</Property>
      <Property Name="RdbConnection Integrated Security" Type="System.String">SSPI</Property>
      <Property Name="RdbConnection Pooling" Type="System.String">>false</Property>
      <Property Name="SsoApplicationId" Type="System.String">AdventureWorks</Property>
      <Property Name="SsoProviderImplementation" Type="System.String">Microsoft.SharePoint.Portal.SS
    </Properties>
  </LobSystemInstance>
</LobSystemInstances>

```

14. **Import the Application Definition File** into the Farm by navigating to SharePoint Central Administration.
15. Click the **Shared Services Provider** on the left hand side Quick Launch Navigator.
16. In the **Business Data Catalog** section click **Import Application Definition File**.
17. Browse to the Application Definition File that you saved in step 13.
18. Click **Import**.

SETTING THE CREDENTIALS FOR THE BDC ENTITIES

Once you have imported the BDC Application Definition, you will need to set permissions on the Entities so that your users can use them.

1. From the **Shared Services Provider Page** choose **View Applications** from the Business Data Catalog section.
2. Hover the mouse over the Application Definition File that you wish to edit, and click the drop down list.
3. Choose **Manage Permissions**
4. Click **Add Users/Groups** and Add the users who will be able to access the Entity using BDC.
5. Choose the **appropriate permissions**. (Most users will just require Execute.)

SSP01 > Business Data Catalog Applications > AdventureWorksLOBSYSTEM > Manage Permissions

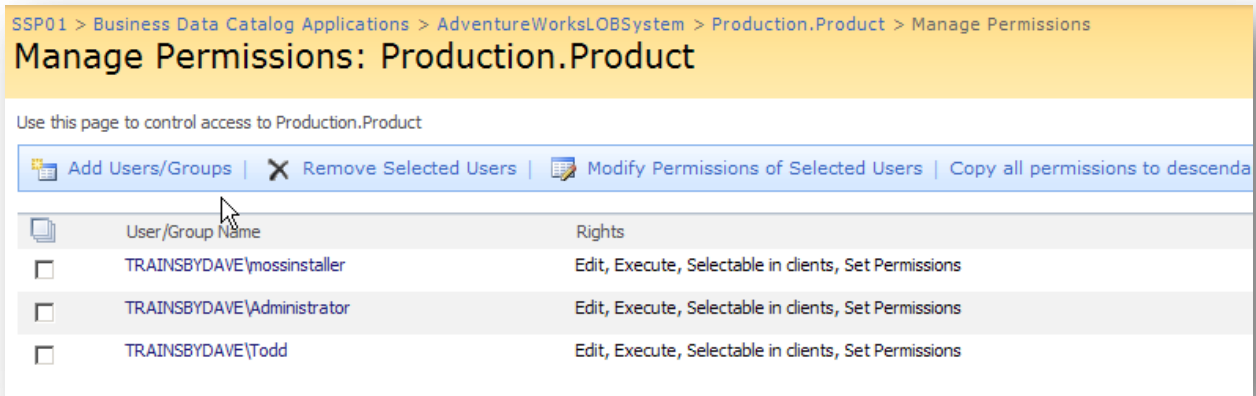
Manage Permissions: AdventureWorksLOBSYSTEM

Use this page to control access to AdventureWorksLOBSYSTEM

[Add Users/Groups](#) |
 [Remove Selected Users](#) |
 [Modify Permissions of Selected Users](#) |
 [Copy all permissions to descendants](#)

User/Group Name	Rights
<input type="checkbox"/> TRAINSBYDAVE\mossinstaller	Edit, Execute, Selectable in clients, Set Permissions
<input type="checkbox"/> TRAINSBYDAVE\Administrator	Edit, Execute, Selectable in clients, Set Permissions
<input type="checkbox"/> TRAINSBYDAVE\Todd	Edit, Execute, Selectable in clients, Set Permissions

- Using the breadcrumb trail navigate back to the **LobSystem** in my example '**AdventureWorksLOBSystem**'.
- Click on your **Entity** which is listed towards the bottom of the page and choose **Manage Permissions**.
- Click **Add Users/Groups** and Add the required Users and set the required permissions on the entity.



ADD THE BDC LIST WEB PART

- To test your **SSO & BDC Configuration**, navigate to a SharePoint Team Site or Page.
- Choose **Site Actions, Edit Page**
- Click **Add A Web Part** in the Left Hand Zone.
- Choose the Business Data List Web Part from the Business Data Catalog section.
- Follow the hyperlink in the Web Part to 'Open the tool pane'.
- Set the Type to be the name of your Entity e.g. **Production.Product** and then click the **Check icon**.
- Choose **Ok**
- You should see your Business Data in the Web Part as shown below:

Production.Product List					
Actions ▾					1 - 20 ▾
ProductID	Name	ProductNumber	Color	ReorderPoint	StandardCost
1	Adjustable Race	AR-5381		750	0.0000
2	Bearing Ball	BA-8327		750	0.0000
3	BB Ball Bearing	BE-2349		600	0.0000
4	Headset Ball Bearings	BE-2908		600	0.0000
316	Blade	BL-2036		600	0.0000
317	LL Crankarm	CA-5965	Black	375	0.0000
318	ML Crankarm	CA-6738	Black	375	0.0000
319	HL Crankarm	CA-7457	Black	375	0.0000
320	Chainring Bolts	CB-2903	Silver	750	0.0000
321	Chainring Nut	CN-6137	Silver	750	0.0000
322	Chainring	CR-7833	Black	750	0.0000
323	Crown Race	CR-9981		750	0.0000
324	Chain Stays	CS-2812		750	0.0000
325	Decal 1	DC-8732		750	0.0000
326	Decal 2	DC-9824		750	0.0000
327	Down Tube	DT-2377		600	0.0000
328	Mountain End Caps	EC-M092		750	0.0000
329	Road End Caps	EC-R098		750	0.0000
330	Touring End Caps	EC-T209		750	0.0000
331	Fork End	FE-3760		600	0.0000

Note that I am currently logged in as Todd who is a member of the Sales Domain Group. If I sign in as a user who is not a member of that group, permission is denied despite the users having access to the site and the entity.

To test SSO is configured correctly. Try and access the site using an account that is not a member of your Domain Group that you configured in the SSO Application Definition. Verify that the users cannot access the data, and then add them to the Domain Group to test SSO. If it works, then SSO is configured correctly.

Financials | News ▾ | Reports | Search | **Sites**

Portal > Sites > TestSSO

Production.Product List

Actions ▾ 1 - 20 ▾

ProductID	Name	ProductNumber	Color	ReorderPoint	StandardCost
1	Adjustable Race	AR-5381		750	0.0000
2	Bearing Ball	BA-8327		750	0.0000
3	BB Ball Bearing	BE-2349		600	0.0000

Microsoft Windows SharePoint

Welcome Todd ▾

Note - Signed in as Todd - Data is displayed.

Welcome Zoe ▾

News ▾ Reports Search **Sites**

Portal > Sites > TestSSO

Production.Product List

Actions ▾

ProductID	Name	ProductNumber	Color	ReorderPoint	StandardCost
-----------	------	---------------	-------	--------------	--------------

You do not have permission to connect to AdventureWorksInstance.

Microsoft Windows SharePoint Services

Sign in as Zoe - Who is not a member of the Sales group. Permissions are denied to the AdventureWorksInstance

Active Directory Users and Computers

sales Properties

Members:

Name	Active Directory Folder
Administrator	trainsbydave.com/Users
Bill	trainsbydave.com/TBDMOSS/Support
Brett	trainsbydave.com/TBDMOSS/Support
Todd	trainsbydave.com/TBDMOSS/Support

Add Zoe to the Sales Domain Group

Select Users, Contacts, or Computers

Select this object type:

Users or Other objects

Object Types...

From this location:

trainsbydave.com

Locations...

Enter the object names to select (examples):

Zoe [Zoe@trainsbydave.com]

Check Names

Advanced...

OK Cancel

Schema Admins Security Group ... Designated administrators...

Welcome Zoe ▾

News ▾ Reports Search Sites

Portal > Sites > TestSSO

Production.Product List

Actions ▾ 1 - 20 ▸

ProductID	Name	ProductNumber	Color	ReorderPoint	StandardCost
1	Adjustable Race	AR-5381		750	0.0000
2	Bearing Ball	BA-8327		750	0.0000

Microsoft Windows SharePoint

SUMMARY

It is worth noting that different environments and permissions can affect BDC and SSO. If you cannot get SSO and/or BDC to work correctly we are more than happy to guide you. However, I hope you found this whitepaper useful as an introduction to configuring BDC & SSO. No doubt there will be some things that I have not mentioned. If this is the case then please let me know so that I can include it in the whitepaper and help other readers. Other Whitepapers and screencasts are available from either <http://www.bdcmetaman.com> or <http://www.lightningtools.com> which may also help you with your configuration.

If you wish to suggest corrections or additions, please email me on the email address listed below.

Kind regards

Brett Lonsdale

brett@lightningtools.com