Securing Decision Support Software

Introduction

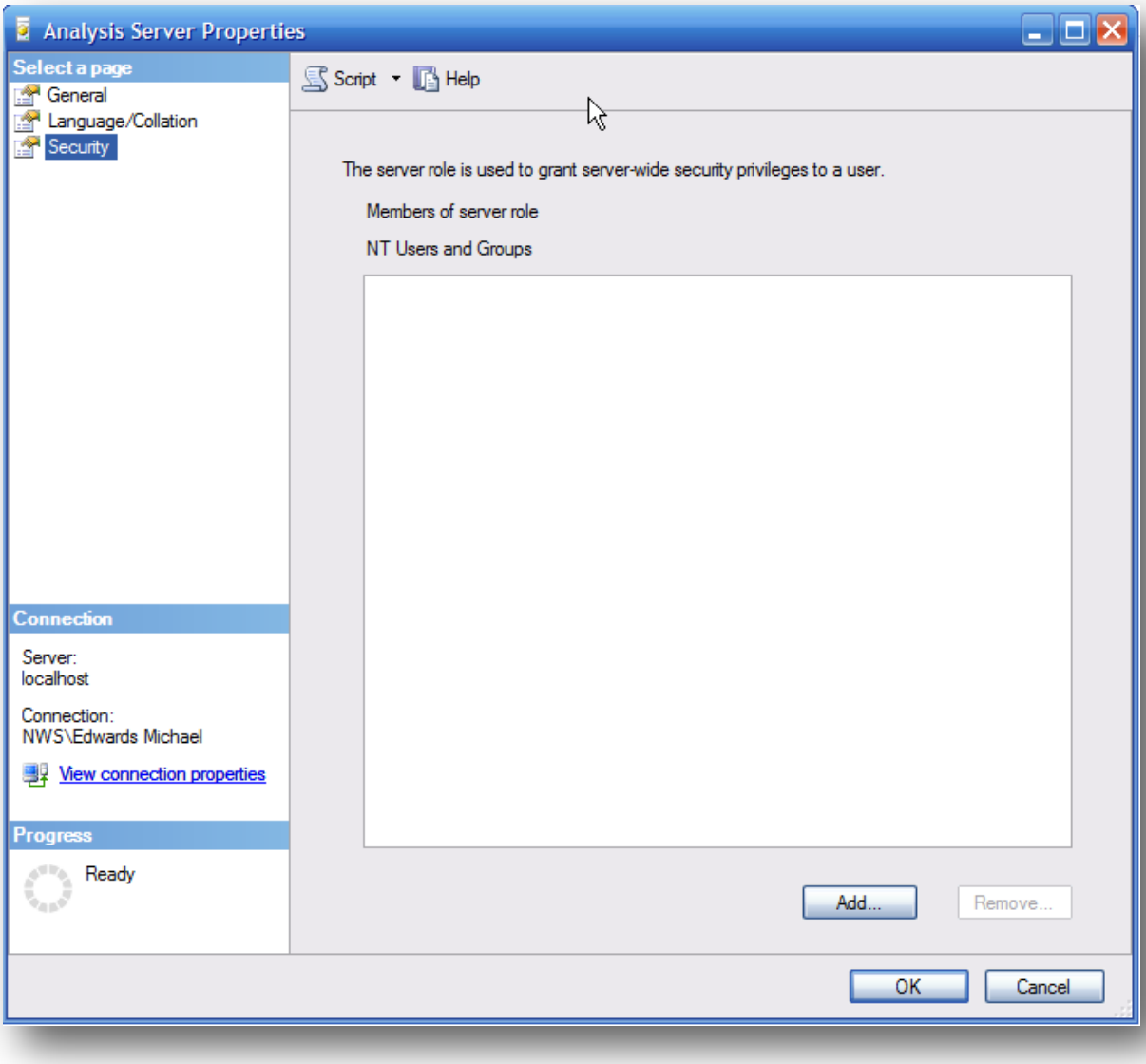
Security in Decision Support Software (DSS) is separate and maintained outside the Logos.NET application. Microsoft Analysis Services strictly uses role-based Windows Authentication to control access to Analysis Services databases and the data within each Cube. The granularity of data access can be fine-tuned from the entire database to individual data elements.

DSS Server Role

First, open **Microsoft SQL Server Management Studio** and select **Analysis Services** as the Server type. Select or type the server where DSS is installed and click **Connect**.

Once you've connected to Analysis Services, right-click on the server name itself and choose **Properties**. There are three options on the left: **General, Language/Collation, and Security**. Choose **Security** to add a user or group to the Server role.

Server-level security includes a single server-level role, which provides complete SSAS access to assigned users[1].



There are two important things to remember when using the Server role:

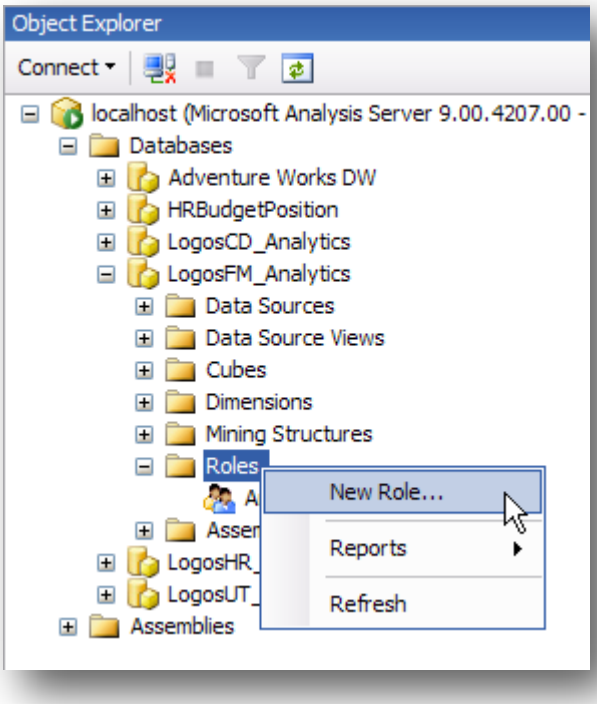
The server role provides complete access to the features and functionality of the entire SSAS Instance; including data and processing.

Users who are members of the local administrators group on the same server as the SSAS instance are included in the server role automatically even though the local administrator group does not appear on the server role list.

[1] Source: http://technet.microsoft.com/en-us/library/cc304417.aspx#

Create Role

To create a role for a specific Analysis Services database, expand the **Databases** folder, expand the **Roles** folder, and right-click on the **Roles** folder and select **New Role.**

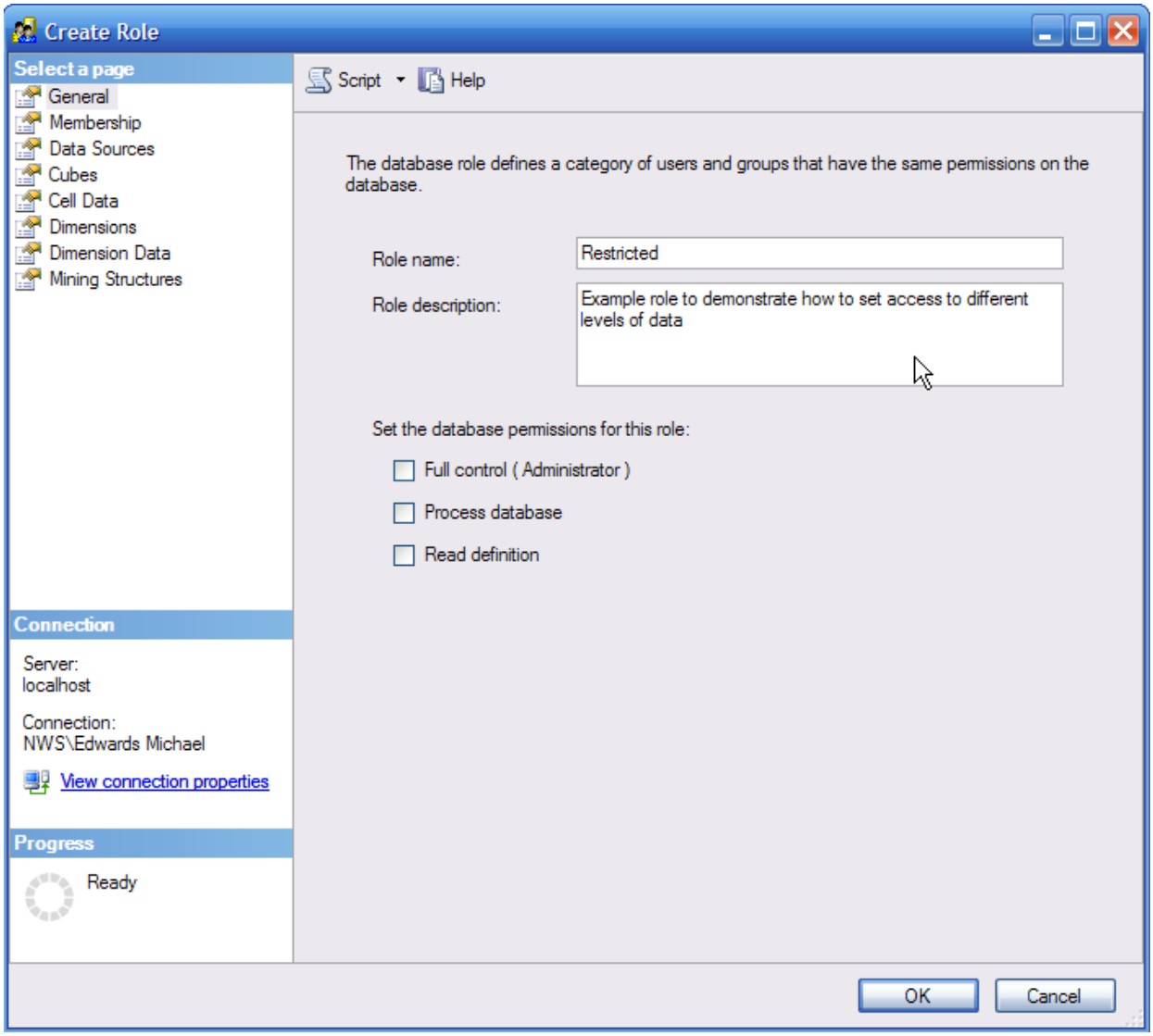


Once you have created the new role, give the role a name and description. There are three checkboxes that control **database** permissions for the role[2]:

> **Full control (Administrator)** Assignment to the Full control role gives complete access to the database, including data, schema, processing, and operations. Administrators can also manage security roles.
>
> **Process database** The Process database role allows SSAS processing. This means a user can be limited to processing the database in which the role is created. However, this option does not give a user read access to the data or definition; read access must be assigned separately.
>
> **Read definition** The Read definition role lets a role member see the full definition of a database; it does not allow a user to have data-access rights or processing rights.

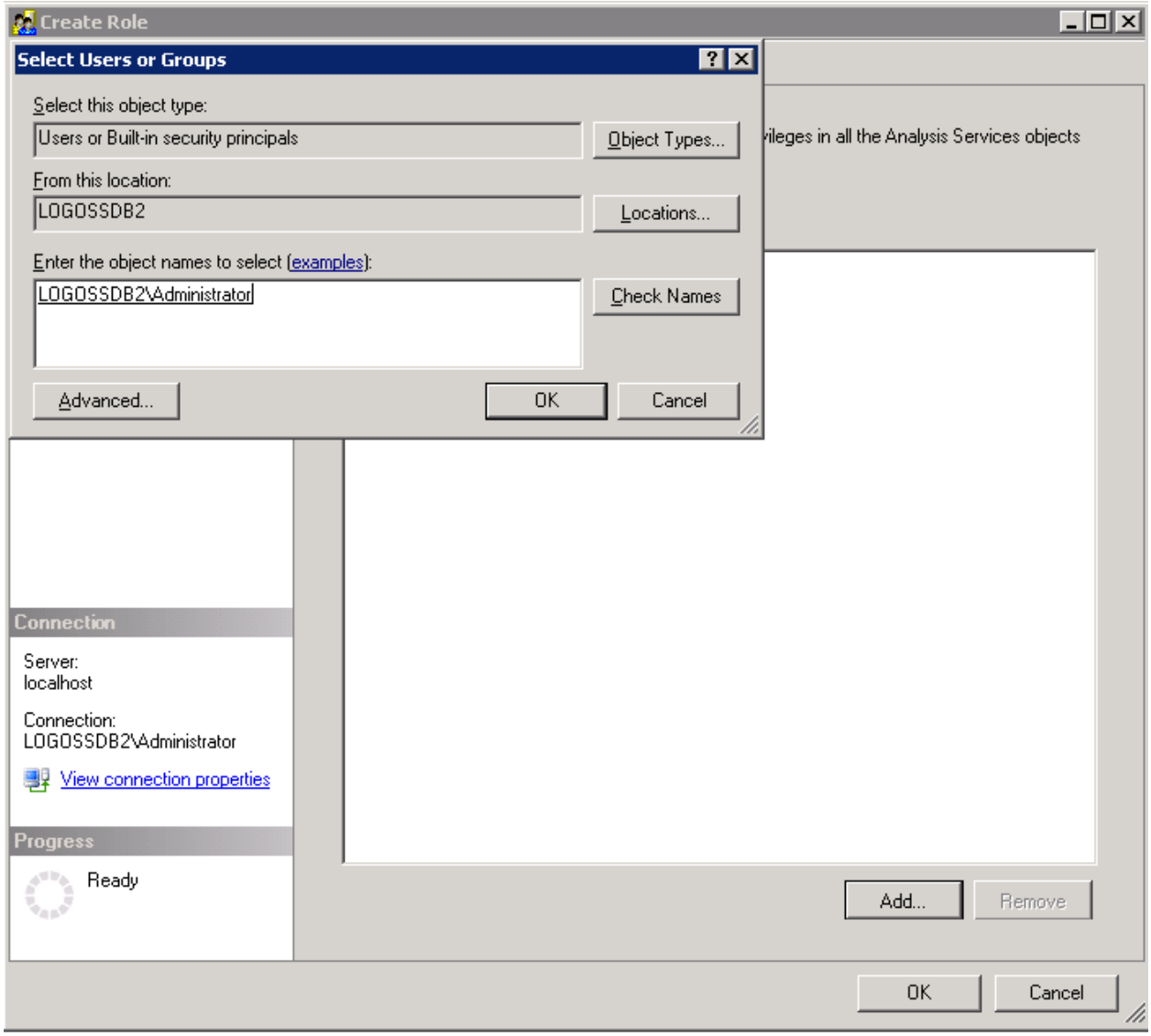
We are creating a role to access data only, so in our case we will not check any of these options.

[2] Source: http://technet.microsoft.com/en-us/library/cc304417.aspx#


Create Role
Select a page
General
Membership
Data Sources
Cubes
Cell Data
Dimensions
Dimension Data
Mining Structures
Script
Help
The database role defines a category of users and groups that have the same permissions on the database.
Role name:
Restricted
Role description:
Example role to demonstrate how to set access to different levels of data
Set the database permissions for this role:
Full control (Administrator)
Process database
Read definition
Connection
Server:
localhost
Connection:
NWS\Edwards Michael
View connection properties
Progress
Ready
OK
Cancel

Adding Users / Groups

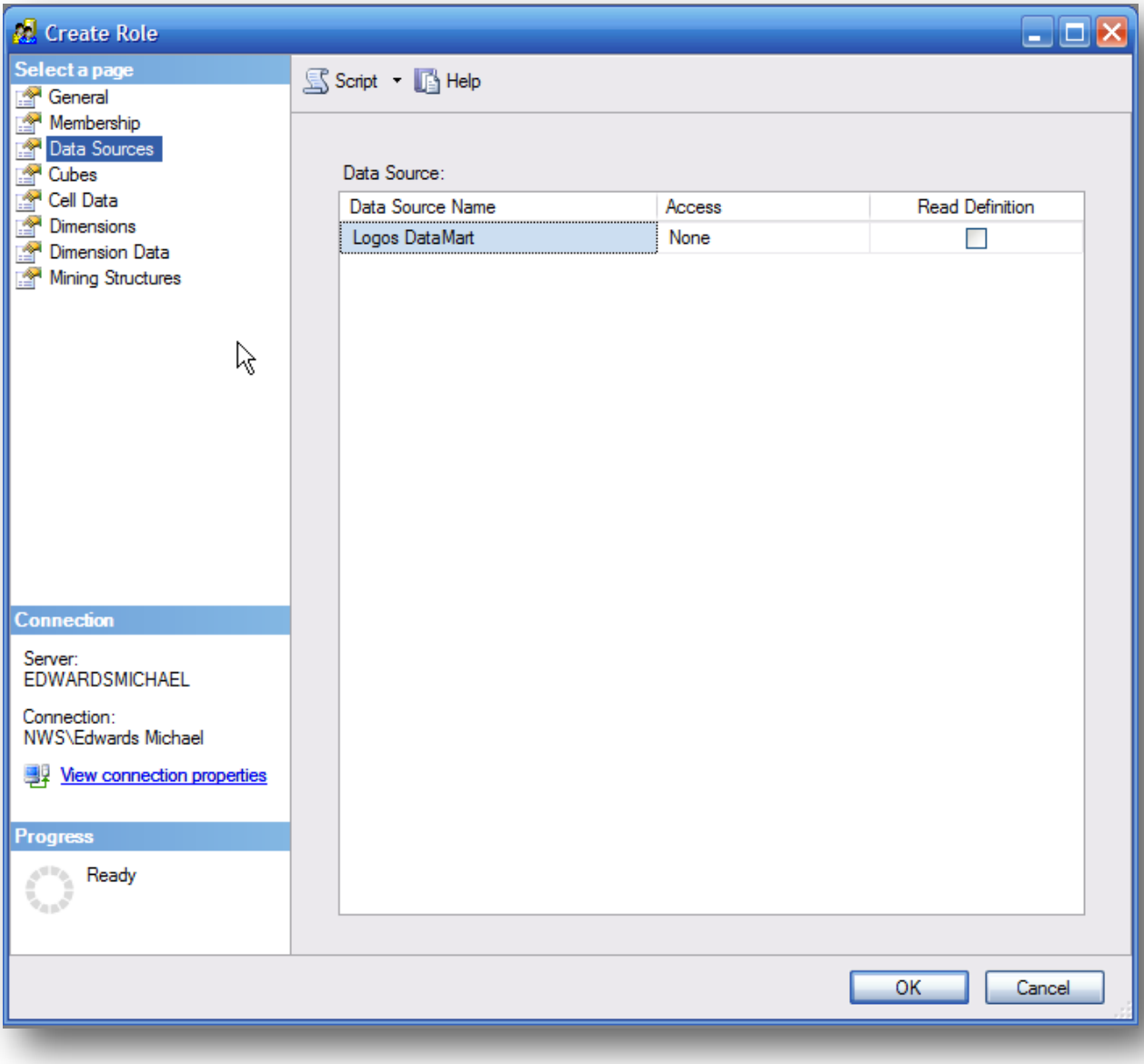
To add a user and/or group to this role, click on the **Membership** page and click on **Add**.



You may have to click on **Locations** to select the correct domain. Type in names or groups, and click on **Check Names** to validate the names. Click on OK to finish adding users/groups.

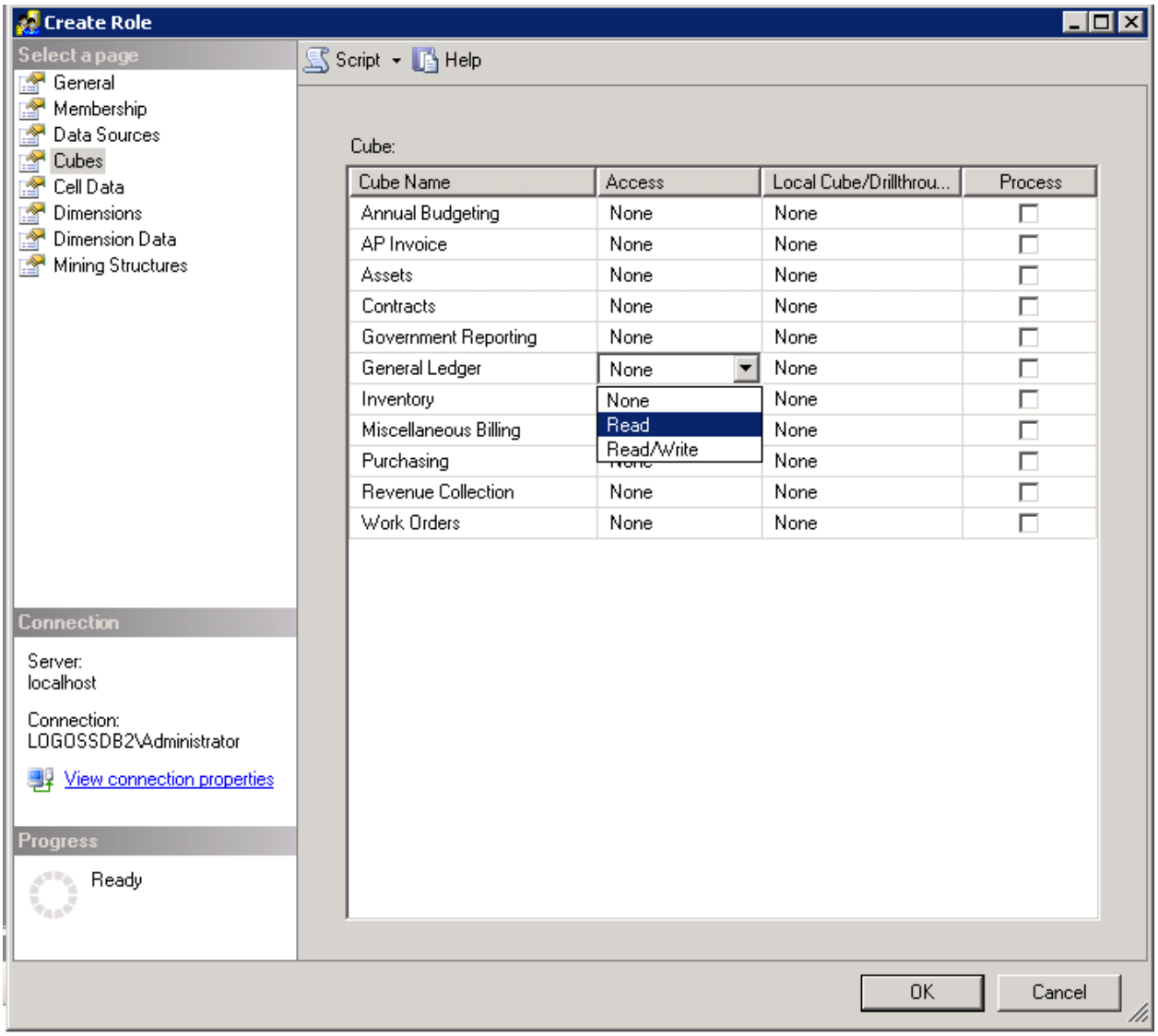
Data Sources

The Data Sources page controls access to the data source for the DSS database. In the Logos Architecture, we do not need to provide access to the data source, as the final data is stored within the DSS database. We can leave this as-is.



Cubes

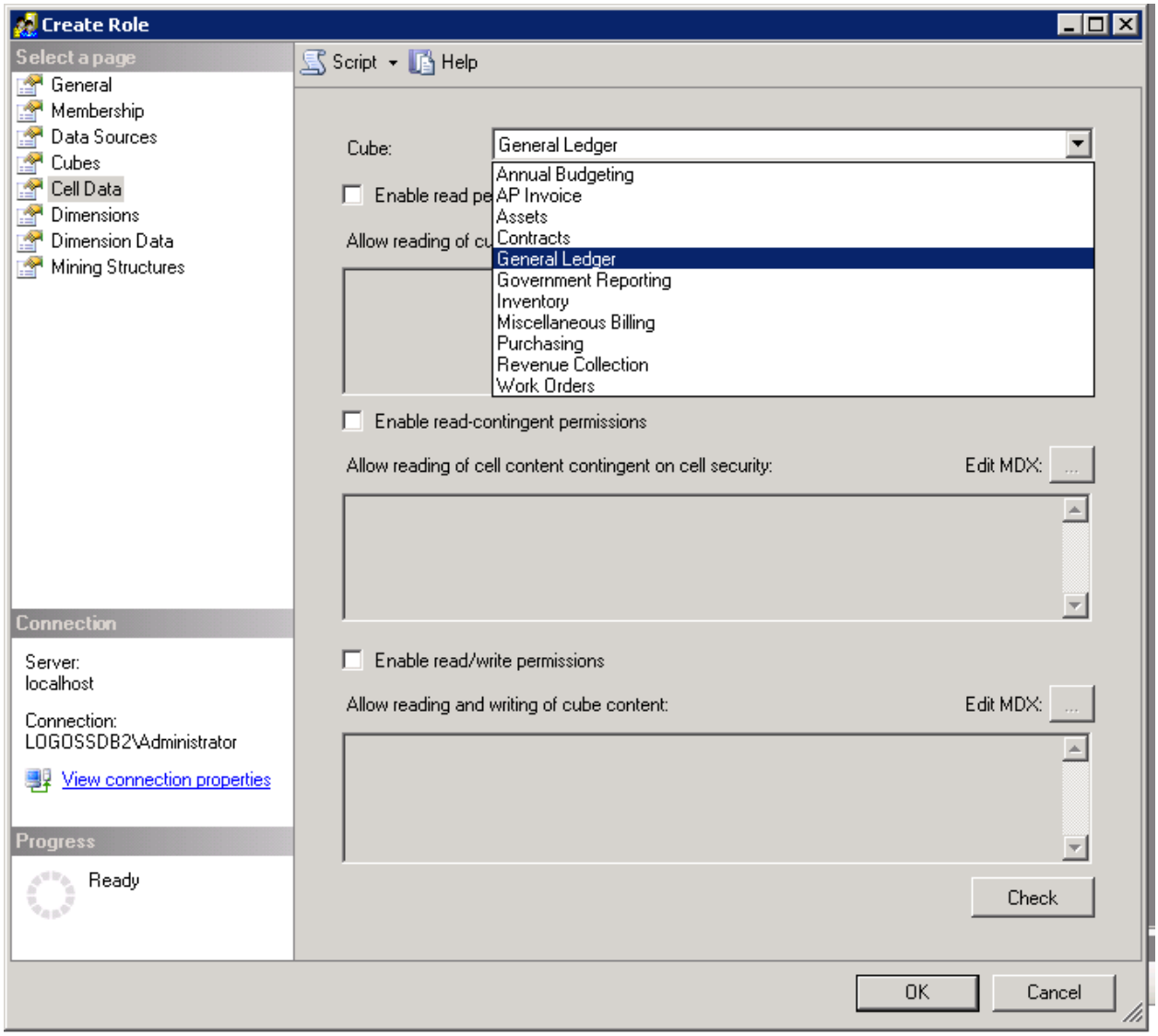
Access must be granted to this role for each appropriate cube. For cubes that are given access, select **Read** access, as at this time we are not allowing write-backs to the database.



Note: You may want to block access to cubes that will not be used by your entity to prevent users from seeing those cubes in the dropdown. For example, the Employee Benefits cube is only usable when Benefits Administration is licensed in HR. This cube will be empty if Benefits Administration is not used. Likewise, the Projects cube and Government Reporting cubes would be empty if Project Accounting and Government Reporting are not licensed.

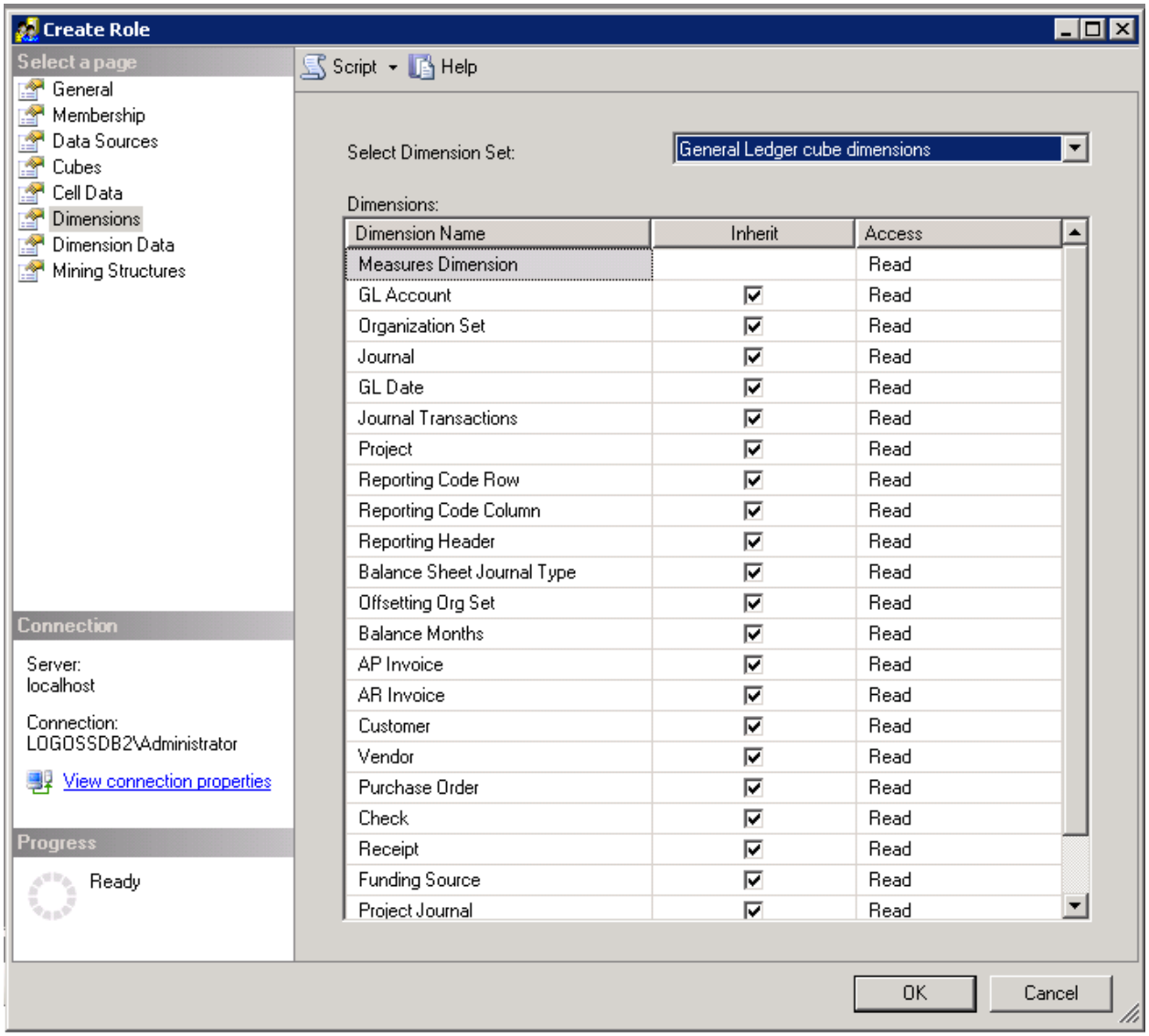
Cell Data

This section is used to restrict access to specific data within the cube. This is done primarily through defining Multidimensional Expression (MDX) queries, which is out of the scope of this basic guide. The default settings can be left in place.



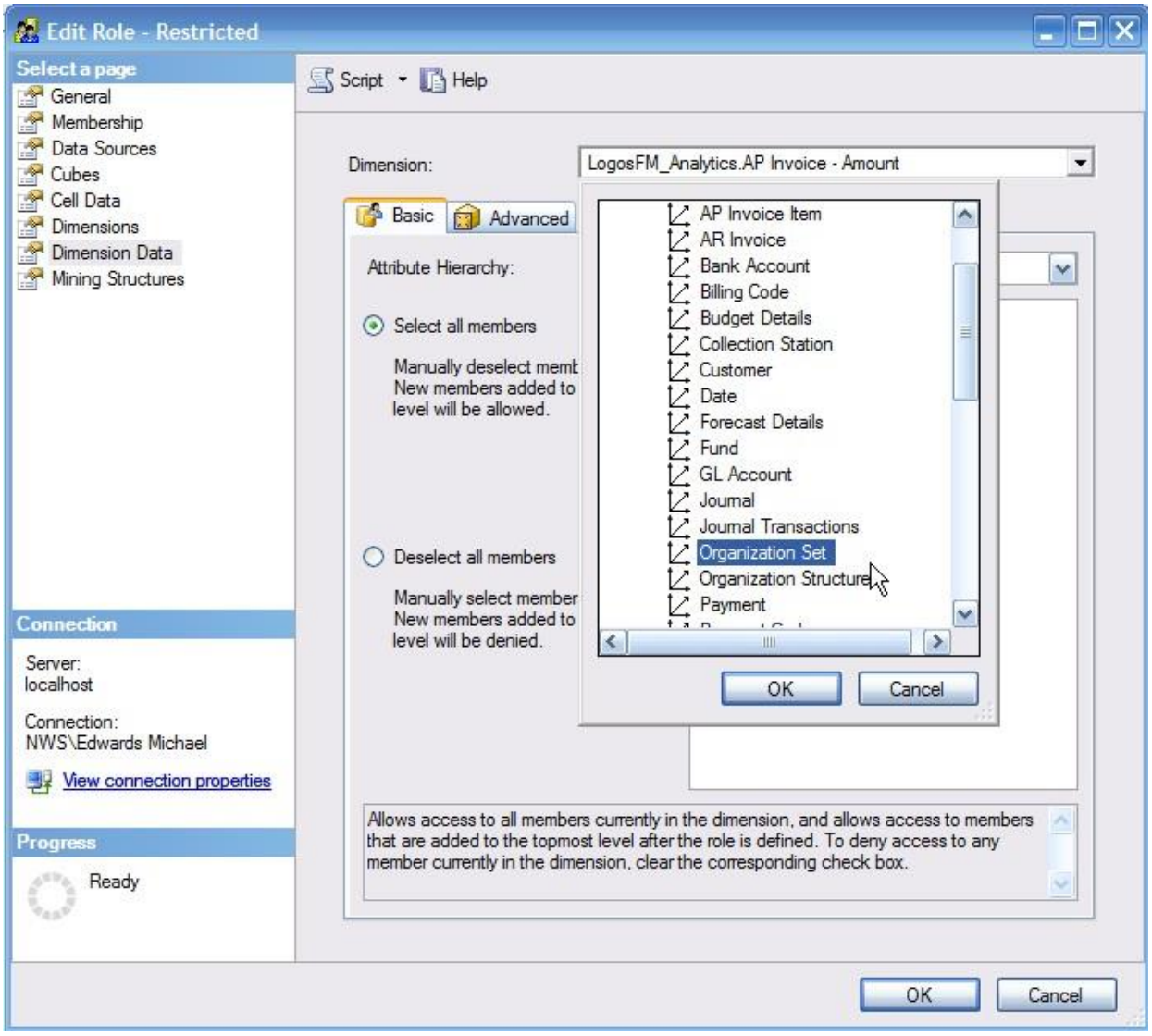
Dimensions

On the Dimension page, you can restrict access to entire dimensions by checking or unchecking the appropriate checkboxes. The **Select Dimension Set** dropdown allows you to select specific cubes this role has access to and restrict the appropriate dimensions.

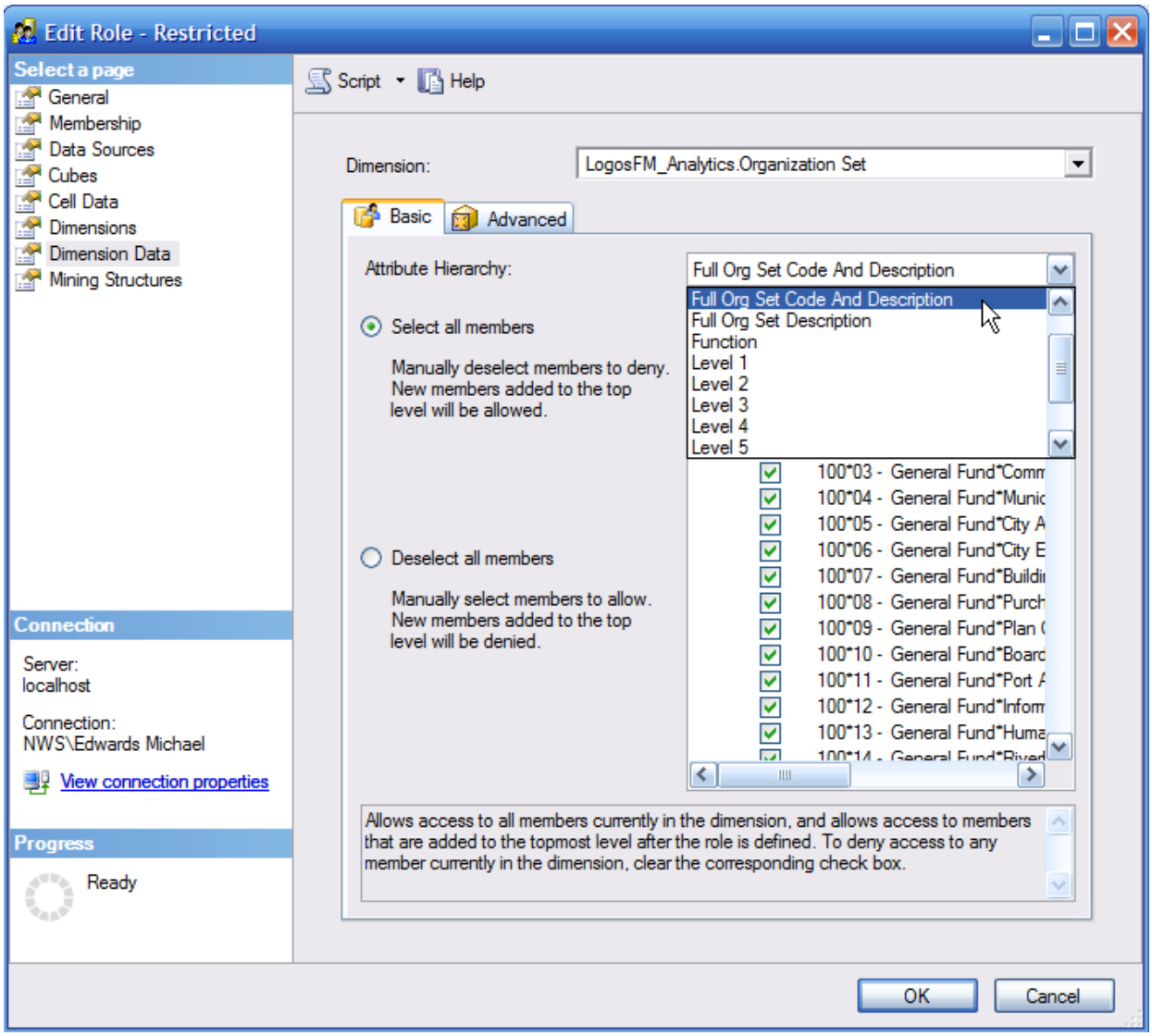


Dimension Data

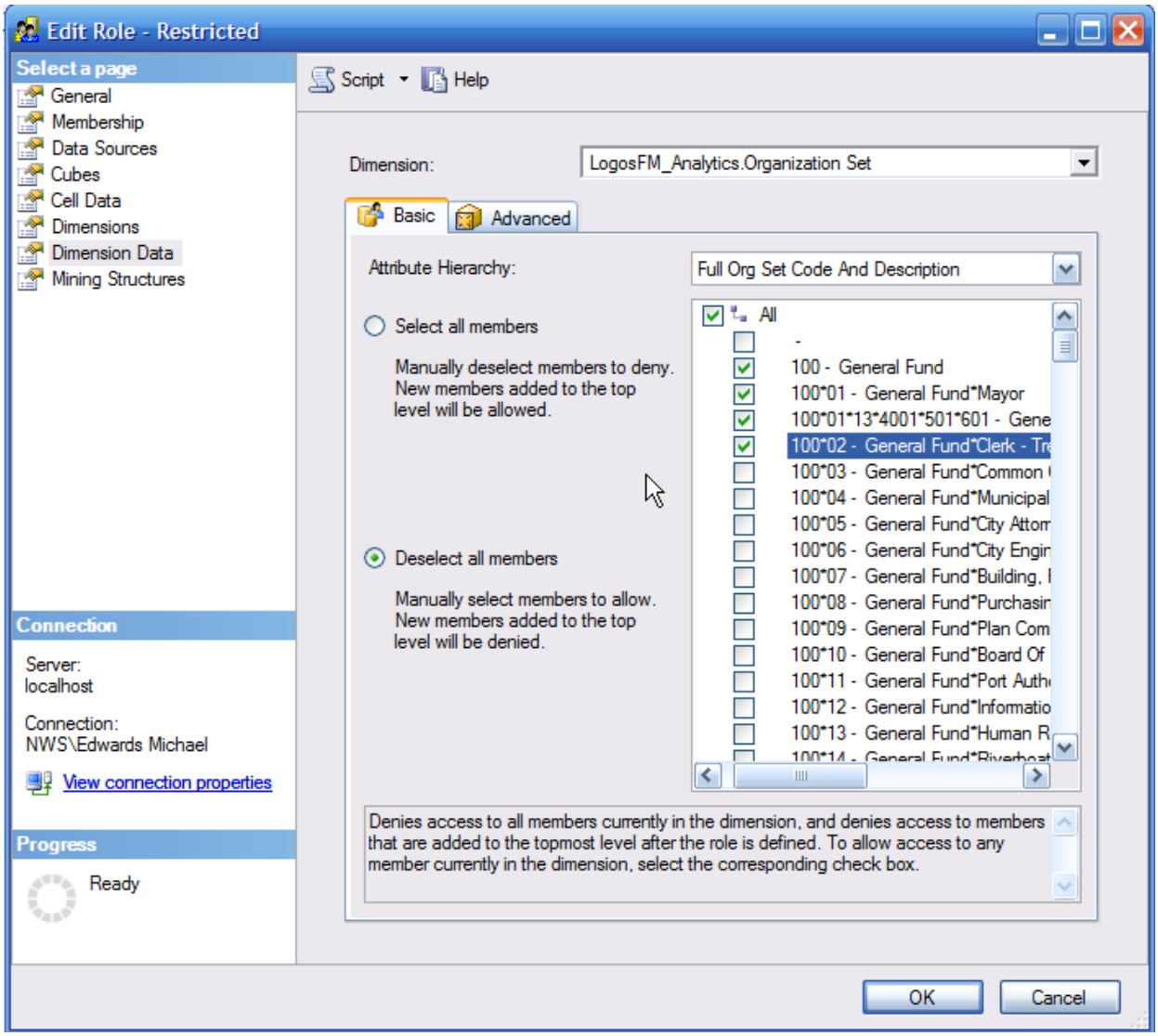
This page allows for limiting specific data within a dimension. First, select the dimension from the dropdown at the top of the page.



Next, select the attribute you would like to restrict. This will provide a list of actual data that can be selected or deselected for this specific role.

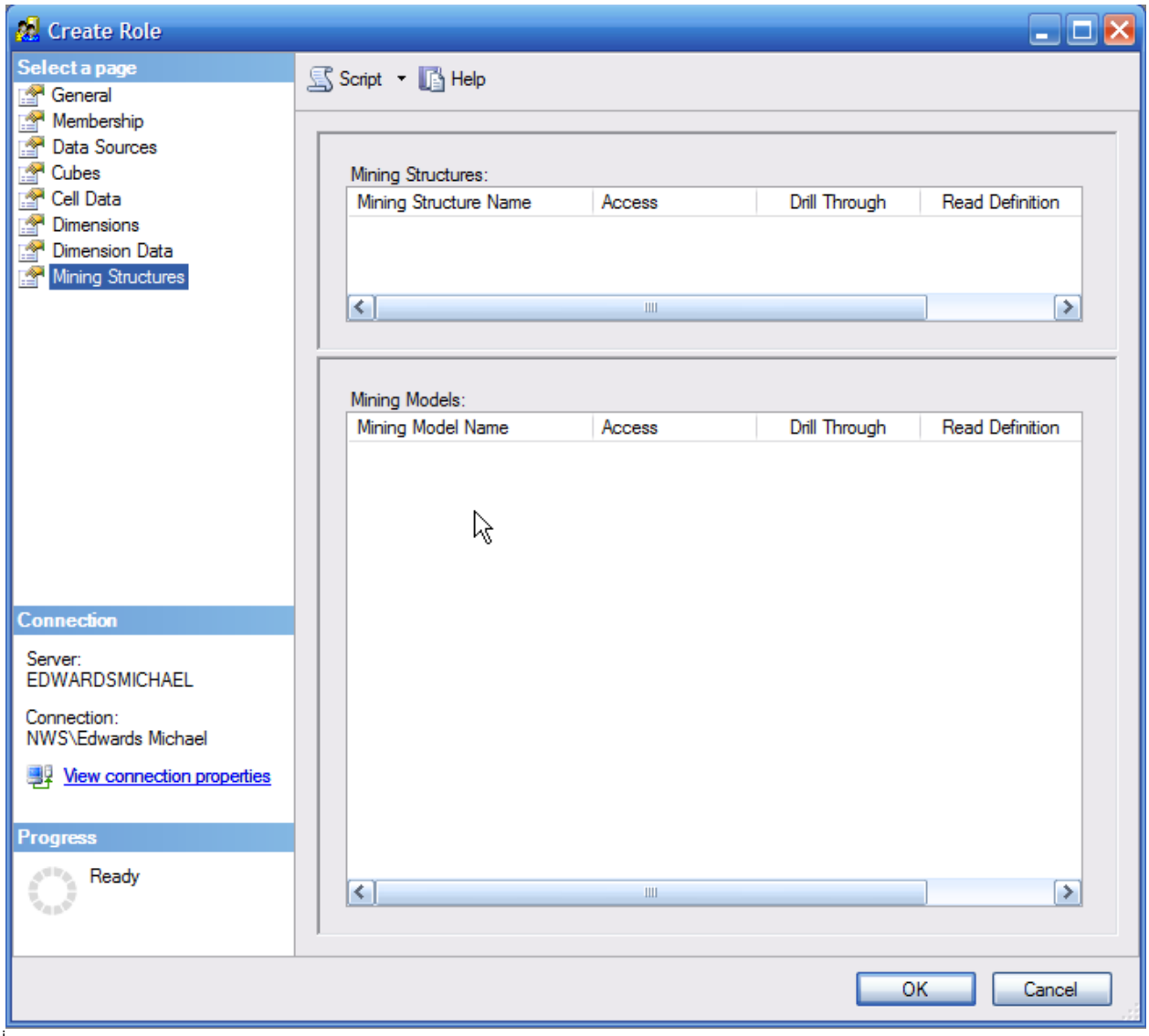


The radio buttons can be used to toggle between selecting members to allow versus selected members to disallow.



Mining Structures

This page can be left as-is. Mining models are not currently used in DSS, and we will address this in future versions as this feature is built-out.



[i]

[i] For more information, visit http://technet.microsoft.com/en-us/library/ms189696.aspx for documentation from Microsoft on the Role Designer interface.