UNIVERSITY OF WISCONSIN

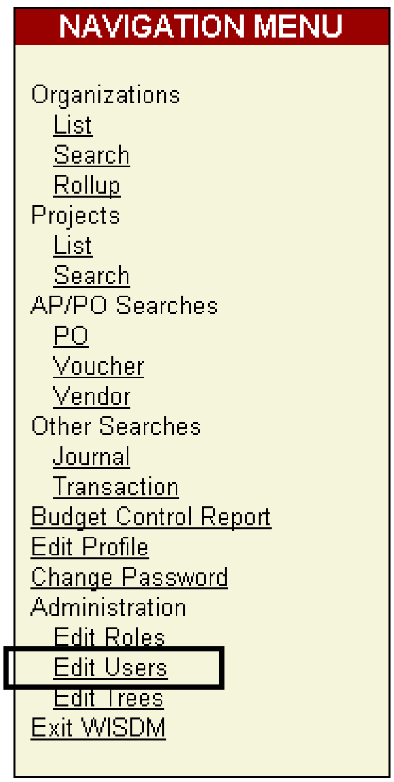
WISDM Administrator Manual

Contents

A primary function of a WISDM campus administrator is to create new user accounts and grant access to his or her business unit to WISDM users from other business units. This manual will walk through setting up a new user, including granting access to the UW Financial Datamart (the GL_STAR and the SFD_STAR). This manual also documents the "Edit Trees" function available in WISDM.

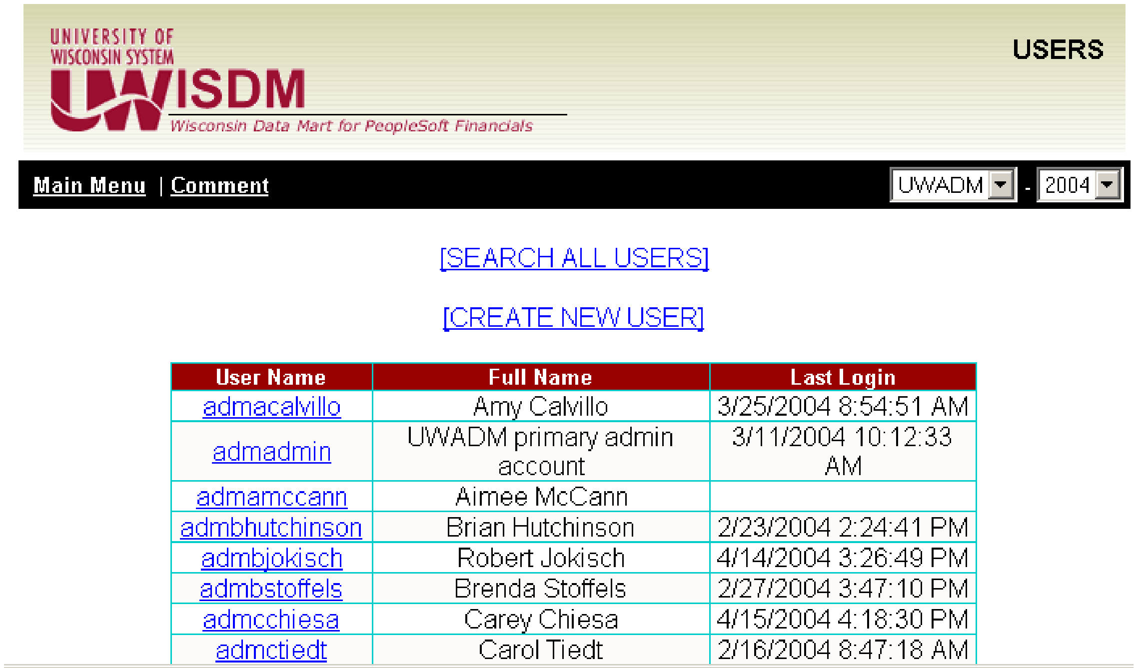
To log into the WISDM website, navigate to http://wisdm.doit.wisc.edu. Sign in with your administrator username and password. All features described in this manual are under the "Administration" section of the Navigation Menu.

Setting up a user

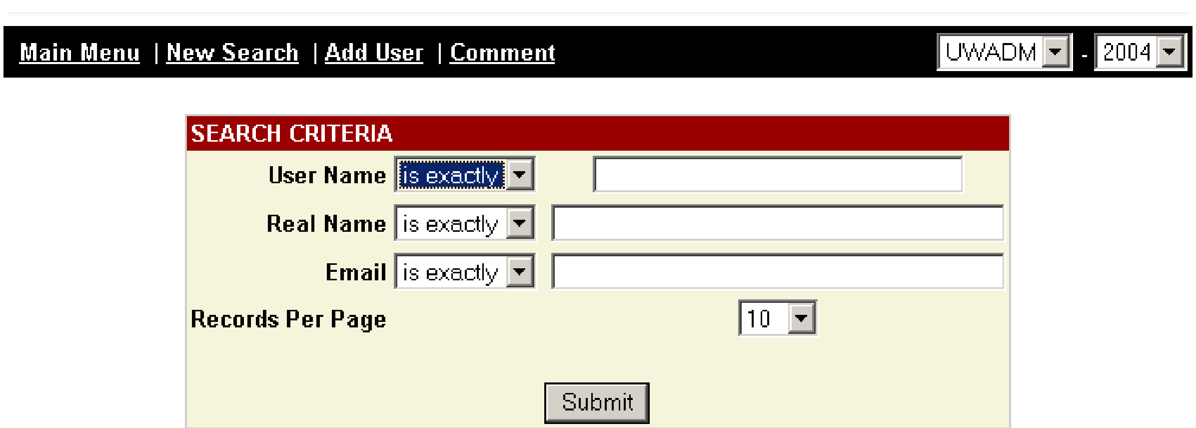


When a new user needs to be added to WISDM, or a current user needs to be given additional access, choose the "Edit Users" hyperlink from the WISDM navigation menu.

When this link is selected, the following screen will appear.

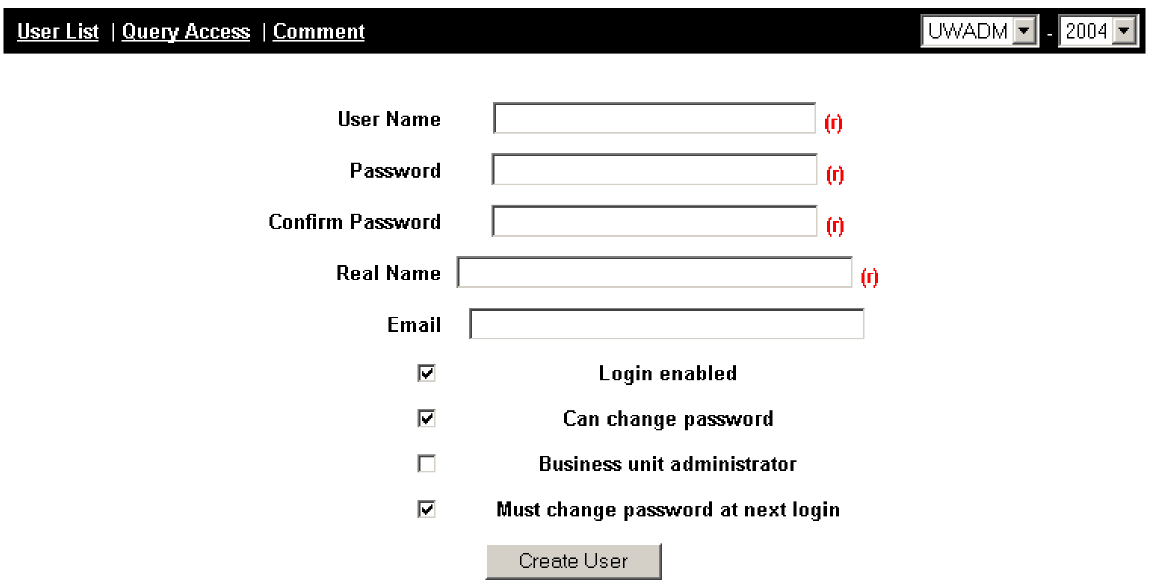


This screen shows all users for your business unit. Before setting up a new user, make sure the user does not have an active WISDM account created. Either search through the list of users (the list is sorted alphabetically by user name) or click on "SEARCH ALL USERS" link. The following screen will appear. (If adding your business to a user from another business unit, use this search to find the user, as they will not show up in the list.)



This search uses the user name, real name, e-mail, or a combination of any of these fields. For example, you could search for a user by entering the three letter campus abbreviation in the "User Name", select "starts with" from the dropdown list, then either view all users of a campus, or limit the results by entering part of the person's real name or e-mail address. Select either "starts with" or "contains" from the dropdown box to ensure accurate results.

If the user does not have a WISDM account, select "Add User". The following screen will appear:



Enter all the fields with a (r) next to them (required field) and check the appropriate boxes:

<u>User Name</u>
Fill in the user name. You MUST use the three letter campus abbreviation as the beginning of the user name. The user name must be at least 4 characters long (3 letters from campus name and at least one additional letter), and cannot be longer than 32 characters. Each campus created their own naming convention for WISDM users.

<u>User Name Requirements</u>
If the individual will use any of the SFS datamart stars, the user name cannot currently include a space or special characters; it can only contain letters and numbers.

<u>Password</u>
The administrator must create a password for a new user. This can be a temporary password or the permanent password. If setting a temporary password, click "Change Pwd Next Login", which forces the new user to change the password before using WISDM. There is also a "Change Password" checkbox. This box should be checked to allow the user to change his or her password at any time. If this box is unchecked, the user cannot change their password.

<u>Password Requirements</u> - Passwords must contain at least one number and one letter, and be at least five characters long. They also cannot contain the username. If the user uses any of the SFS datamart stars, the password cannot start with a number or special character, or contain a space.

Complete the rest of the screen for the new user, and then click on the "Create User" button. The user now has an account in WISDM. However, rights must be granted to the user before they can view information in WISDM.

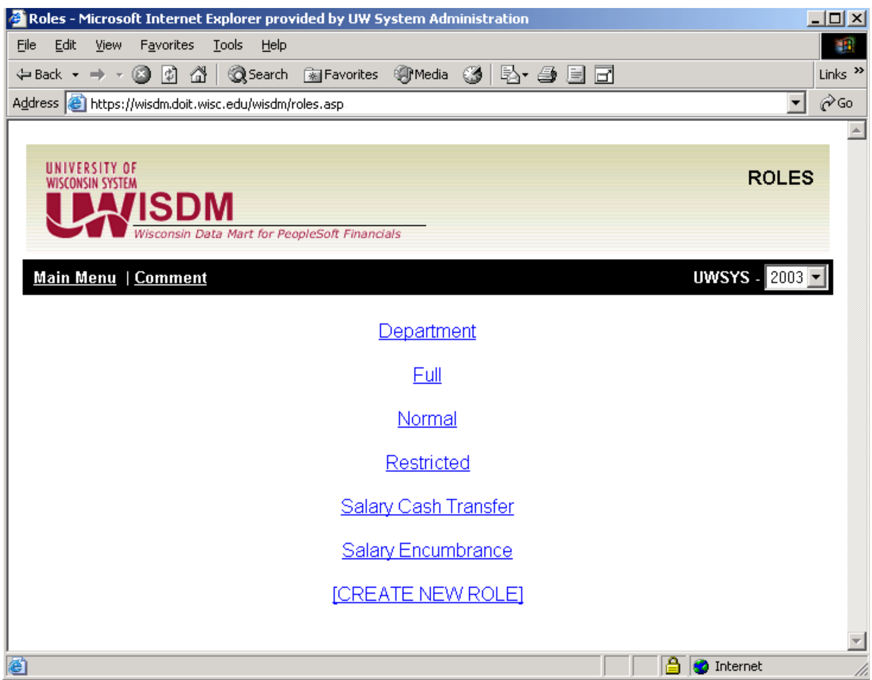
Granting Rights in WISDM

When granting authorizations in WISDM there are two parts to determine:

- What searches and information should the user be able to see?
- At what level should these searches be granted?

Roles

Each business unit administrator can create new roles for their campus and assign rights to those rights. What information is seen in WISDM depends on the rights granted within the role, and what searches are available. For example, if a user needs access to detailed salary and fringe information in WISDM, they need to be granted a role that includes "Payroll". If the "Payroll" right is not granted within the role, the user will not be able to see detailed payroll information. "Full" is one of the roles that, as programmed, has access to payroll data, since "Payroll" is checked. To see which roles are set up for your business unit, select "Edit Roles" from the main menu. You will see something similar to the following:



Select one of the roles, and it will show what rights are granted to a role. When the "Full" is selected here, the following screen appears:

WISDM Administrators can create new roles for their users, then grant rights to these roles based on what the users need. Once user rights are granted, the user can access the information, for which you granted access, immediately in WISDM.

It is important to know that when a role is changed by either adding or removing rights, this affects all users assigned to that role. For example, if I unchecked the “Transaction Search” from the “Full” role above, every user assigned to the “Full” role would lose the ability to perform the “Transaction Search”. Conversely, if a new right were added to a role, every user assigned to that role would be able to use the features granted by the new right. No work is needed with each WISDM account that is assigned to the particular role.

WISDM allows roles to be granted at different levels. The administrator has the responsibility to ensure the proper level is granted to the user. The levels of security include:

Business Unit – All information for entire business unit
Fund – All information for a specific fund

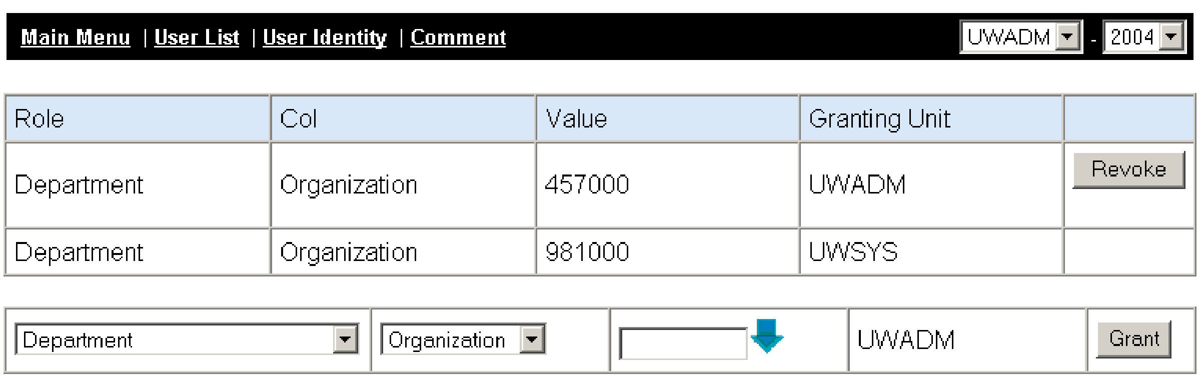
Manager – All information for a specific manager
Organization – All information for a specific org code
Prin. Inv. – All information for a Principal Investigator
Project – All information for a specific project.

When using the Organization level, you can use individual department ID's, or else other tree nodes within your Authorization tree. The tree seen here is the Authorization Tree for UWSYS:

A user can be granted either a single department (101000) or a tree node (PRESIDENT). If PRESIDENT was selected, the user would have access to the four departments listed under this tree node.

These levels work along with the roles to create authorizations for users. The roles define what searches can be used within WISDM, while the levels determine the information that will be returned.

When "User Rights" is selected from the "Create User" screen, the following screen is seen:



Press the blue arrow to view choices from the type of rights granted. If you are granting access based on a particular fund, and press this arrow, a list of all available funds will be seen.

Payroll Interface Specific Setup

With the implementation of Payroll Interface, several searches are available in WISDM to display payroll-specific date. A user must have the appropriate rights granted to use these searches. These rights are the "Salary Encumbrance Searches", "Salary Payment Searches" and "SFD Transaction Search". If these rights are not granted, these searches will not be seen by users. In order for these searches to work appropriately, the "Payrolls" right should also be included in any role that grants one of these three rights.

There are also two new roles available "Salary Encumbrance Application" and "Salary Cash Transfer". These roles give users access to use the new applications that reside within WISDM.

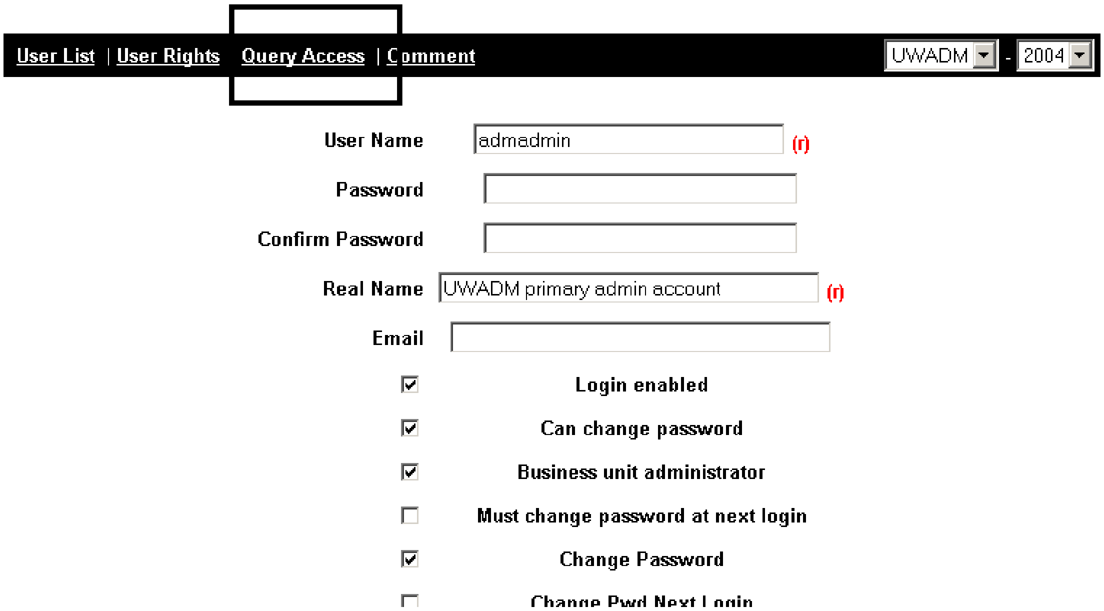
Row Level Security

Row level security is security at a record level that allows users to view only those records that match their security profile, ***no matter the search criteria***. Row level security setup does not affect the functionality of the WISDM website. The WISDM web application essentially is set up with row level security, only allowing users to see specific data, whether it is a division, fund, PI, or entire business unit. It is necessary to set up row level security if the user will be using Brio, or another query tool, to view information from the GL_STAR_FACT table or the SFD_STAR_FACT table. In the future, as more stars are added to the data warehouse, additional row level security will be implemented, and access to these stars will be granted by WISDM administrators.

Currently, for purposes of the GL_STAR_FACT table and SFD_STAR_FACT table, row level security means that the information available to query is limited by business unit. Just like WISDM, the business unit administrator can only grant access to their own business units. Other business unit WISDM administrators grant access to additional business units.

If the row level security setup is not completed, the user will not see results when querying the GL_STAR_FACT or the SFD_STAR_FACT tables.

To establish row level security for a user, go back to the user list (or search) page and select the user. The following screen will appear after you select the user.



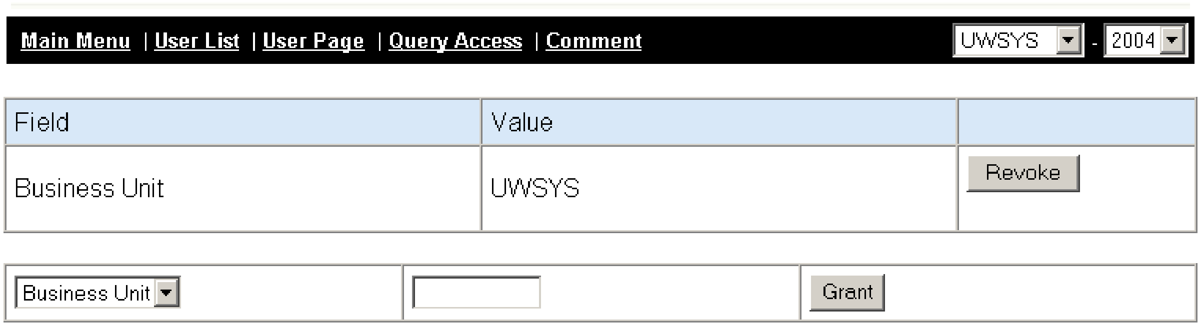
From this page, choose the "Query Access" link on the top of the screen and the following screen will appear.

Enter the user's SFS login name, and click on the star(s) the user needs to query. In the above example, only two selections are available, the GL Star and Aggregate Stars, and the SFD Star. (UW-Madison has additional stars seen on this page.)

GL Star and Aggregate Stars - This selection will allow the user to use the GL_STAR_FACT, the UNIT_PERIOD_SUMMARY_STAR_FACT, the PERIOD_SUMMARY_STAR_FACT, and the BEGINNING_BALANCE_FACT, and the related dimensions.

SFD Star - This selection will allow the user to use the SFD_STAR_FACT, which will allow the user to view detail salary and encumbrance data, and the related dimensions.

After the appropriate selections are made, click on save, then choose the "Row Level Security" link from the top of the screen. This will open the following screen.



Enter the business unit in the “Value” field, then press the “Grant” button, and the business unit will be added to the person’s access. There is not a dropdown list, so type the business unit in correctly. Also, make sure to enter the business unit in UPPER CASE.

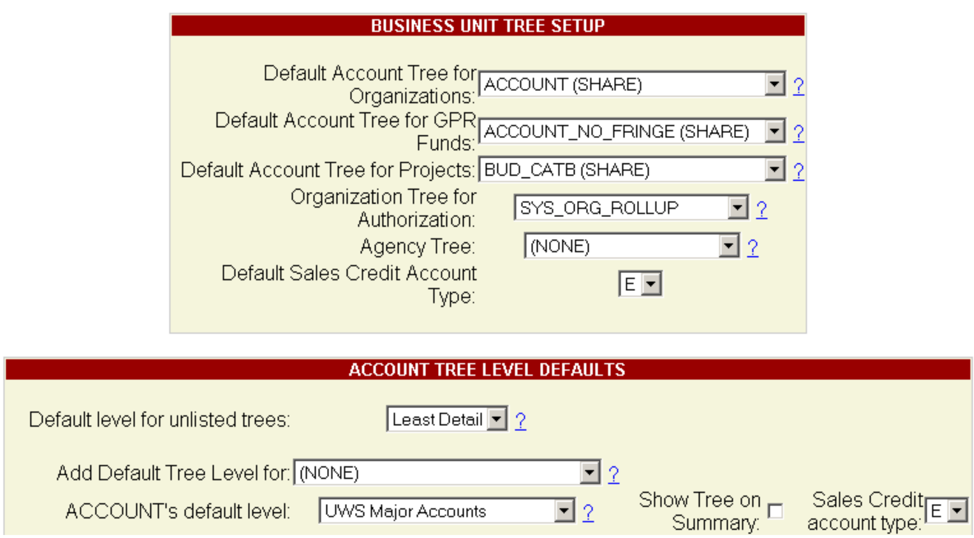
Make sure the user understands row level security in Brio. If the user creates a query in Brio, and limits the query by business unit, they will see all the business units in the limiting criteria. However, they may or may not see the data for the business unit, depending on their rights granted in row level security. Users should still limit their query with the business unit for performance reasons.

Edit Trees

The system administrator has the ability to set up tree defaults in WISDM, which include:

- Setting default trees that first load when viewing data, depending on fund type
- Setting up default trees for authorization
- Setting up how sales credits appear in summary reports (either revenue or expense)
- Setting up which trees are available to users in the dropdown list

These items are set up under the “Edit Trees” link from the main page. When you click on this link, the following appears:



To change your tree setup, choose a different setting in the list boxes. The page will reload and save your changes. The first choice in some lists is **NONE**. If you see **INVALID** after the tree name in the list box, choose a new tree . Parts of WISDM will not work correctly if an invalid tree is selected.

Setting up default trees

Account Tree for Organizations - This account tree is used as the default for summary reports for organizations. This includes Department Only and Both (department and project) reports. If you choose **NONE**, WISDM will use the default tree of BUD_CATB.

Account Tree for GPR Funds - This account tree is used as the default for GPR fund based summary reports. If you choose **NONE**, WISDM will use whatever account tree for organizations you specify (if you do not have an account tree for organizations set, the account tree for GPR funds will be BUD_CATB).

Account Tree for Projects - This account tree is used as the default for summary reports for projects and groups of projects when WISDM cannot find an appropriate tree using your agency tree. If you choose **NONE**, WISDM will use BUD_CATB.

Organization Tree for Authorization - This organization tree is used for authorization purposes only. You can use nodes from this organization tree when you grant access to users. If you choose **NONE**, you can grant access by single DEPTIDs only.

If you set up an organization tree for authorization, the nodes will not be available in a dropdown list; you will be able to type the tree node values when granting access to these nodes. If a tree node is misspelled, no access will be granted, but the system will not let you know the tree node is misspelled.

Agency Tree - This is a PROJECT_GL tree in SFS. These trees are not copied to WISDM. WISDM uses this tree to select agencies, or default account trees, for summaries of projects. If you choose **NONE**, WISDM will use your default account tree for projects for all project summaries.

Account Tree Level Defaults

These settings allow you to choose the default drill down level for a tree when viewed in a summary report. To add a default drill down level for a tree, select the tree in the "Add Default Tree Level" list. The page will then reload and the tree will be listed below the list with a list box with all the available levels of that tree. So set a default, select a level in the list and the page will reload and set that level to your new default. To remove a default level, select **NONE** from the tree's level list. The level selected will be set for all users within your business unit, unless they set a specific level for the tree in their personal options.

Add Default Tree Level - This is to set a default drilldown level for an account summary report. If the levels are not named in WISDM, you will see numbers, with the lower the number meaning more detail. Individual users can override this by setting their own level preferences for individual trees and all other trees (either most detailed or least detailed)

Default Level for Unlisted Trees - This is to set a default drilldown level for an account summary report on account trees not listed on the Business Unit Tree Setup page. If you have an account tree custom default level in your business unit profile, you can have the drilldown level default to the highest available drilldown level or the lowest available drilldown level. Individual users can override this preference.

Show Tree on Summary – This limits the number of trees available to your users. When you select “Show Tree on Summary”, only those trees are available to your business unit’s users. This feature can be useful if a campus uses a few trees and does not want to have the users scroll through many trees when looking for one. It can also help lessen the confusion for users when determining which tree to use. However, users cannot view any other trees than the ones specified here.

Sales Credit Account Type - This is to set how sales credits will appear in WISDM. The choices are R (revenue) or E (negative expense). This can be specified by tree, or left as default for all trees.