Enterprise Content Management: Administrators Training Guide

Prepared by:

U.S. Department of Agriculture

Office of the Executive Secretariat

Rural Development Mission Area

October 2006

Acknowledgments

This training guide has been prepared by Bruce G. Bundick, Kathy Anderson, Doris Kitchings, Kathleen Valdez, and Ed Koenen. Much of the material has been adapted from materials previously prepared by QFlow Systems, Inc. and the ECM Team.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Introduction to the ECM System

Enterprise Content Management: Overview

The Enterprise Content Management process allows users to manage the process of receiving, responding to, and tracking incoming correspondence. The application is web-browser based so users can access the system and perform work from any location. The diagram below shows the system architecture for the new application.

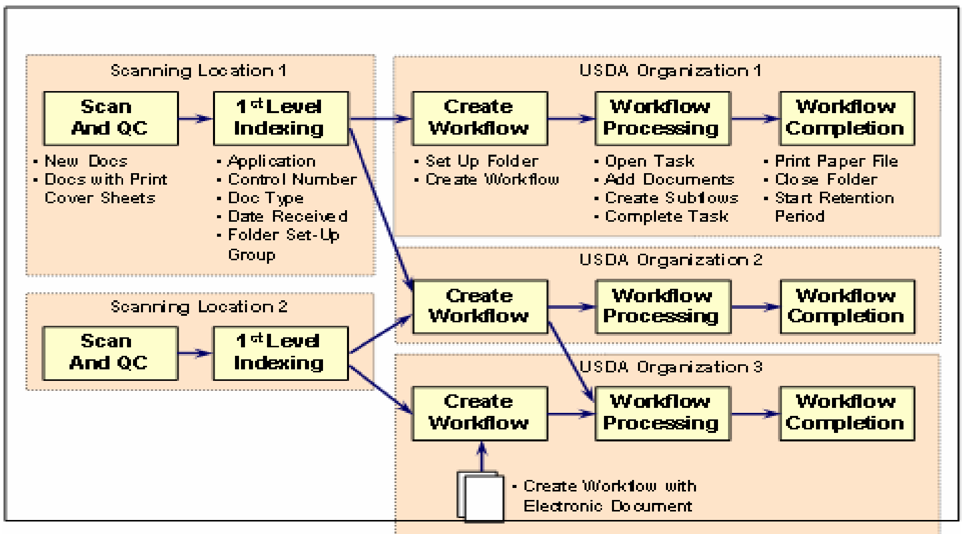


Figure 1: ECM Business Architecture

Documents are scanned into the system from a USDA scanning location. USDA may have any number of scanning locations. The scanning operator performs a Quality Control check. The operator enters some basic document index information. Document indexes categorize the correspondence and forward it to the group responsible to set-up the folder for the document. The system then transfers the documents to the centralized document repository at USDA. Once the document is stored, the system starts the workflow process.

The workflow process routes the document through necessary processing steps that may include the following:

- Set up a new folder with the scanned document.
- Create the workflow list of tasks and assignees.
- Route the folder through the workflow tasks for processing:
  - Research the issues.
  - Create a draft response letter.
  - Route the draft response letter for revision and approval.
  - Create the final response letter and print on agency letterhead.
  - Obtain the necessary signature.
  - Mail the response letter.
- Finalize the Correspondence Management information.
- Close the folder.
- Archival tasks.

The actual tasks that are performed depend on the requirements of the document. The Folder Owner determines the actual workflow tasks and assignees necessary to respond to the incoming correspondence. The system provides capabilities that allow each individual to manage his or her workflow tasks using their inbox. Workflows can be monitored by individuals wishing to see a folder's current status and and/or to help ensure timely completion.

In addition to accessing the system to process correspondence, authorized users may search the system for documents and folders. Searches can be performed on the document or folder indexes. Alternatively, full-text searches can be performed to find all documents that contain specific words or phrases.

Preparing to Use ECM; A Word About...

Web Applications

Internet Explorer Configuration for ECM

Timing Out of the Application

Folder Status (Suspended Folders)

Active, but "Stuck" Folders

Back Button

Microsoft Office Integration

Hints and Suggestions

Web Application

ECM is a web-based application. It does not depend upon special software on the user's computer, other than the standard browser Internet Explorer. (Note: The application does require Java and Microsoft.Net Framework software. This software is part of the standard configuration on many USDA computers, and if it is not present, it attempts to load automatically the first time the application is accessed.)

As a web-based application, users may access ECM from any computer that has access to the USDA internal network, either through direct physical access or through a VPN network connection. Users should understand, however, that the changes made on the local browser screen are usually not transmitted to the application servers until the changes are saved or otherwise "committed." If an application window is closed before it is saved, or if the application times out, all unsaved changes are lost.

Internet Explorer Configuration for ECM

Pop-up Blocker

ECM makes extensive use of the "pop-up" window, a special kind of browser window that appears over the top of the main application window. In order to successfully work within the ECM application, the user cannot "block" pop-ups. A pop-up blocker may be enabled by default by Internet Explorer (IE), by many accessory browser tool bars (Google, Yahoo, etc.), and by some types of security software. Users and/or their administrators must add the ECM URL to the local pop-up blocker "safe list," or remove or disable the pop-up blocker. (Examples use IE version.)

Select the **Tools** menu from the tool bar. Select the **Pop-up-Blocker** submenu. Select **Turn Off Pop-up Blocker** to disable the Pop-up blocker, or select **Pop-up Blocker Settings** to configure the Pop-up Blocker for ECM use.

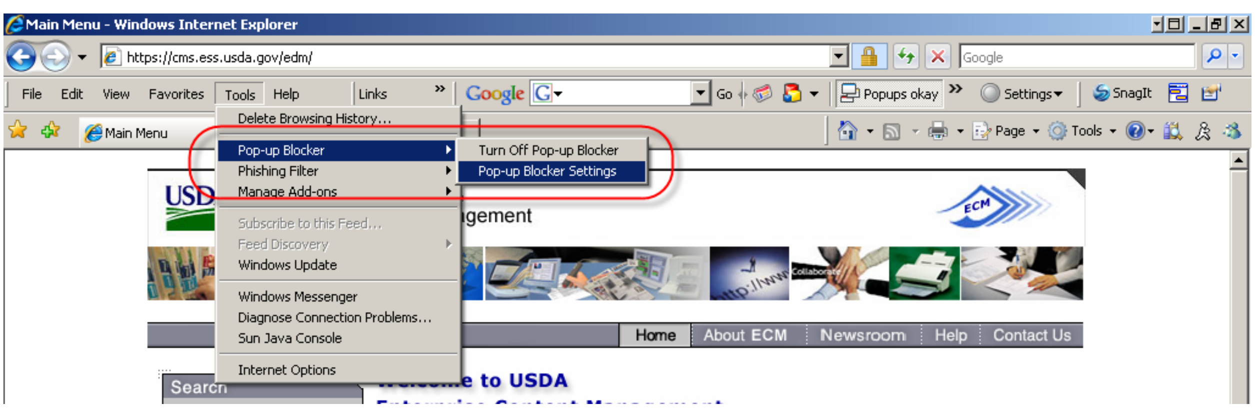


Figure 2: Internet Explorer Tools Menu (Turn Off or Configure Pop-up Blocker)

To configure the Pop-up Blocker, select **Pop-up Blocker Settings**. The **Pop-up Blocker Settings** window will open.

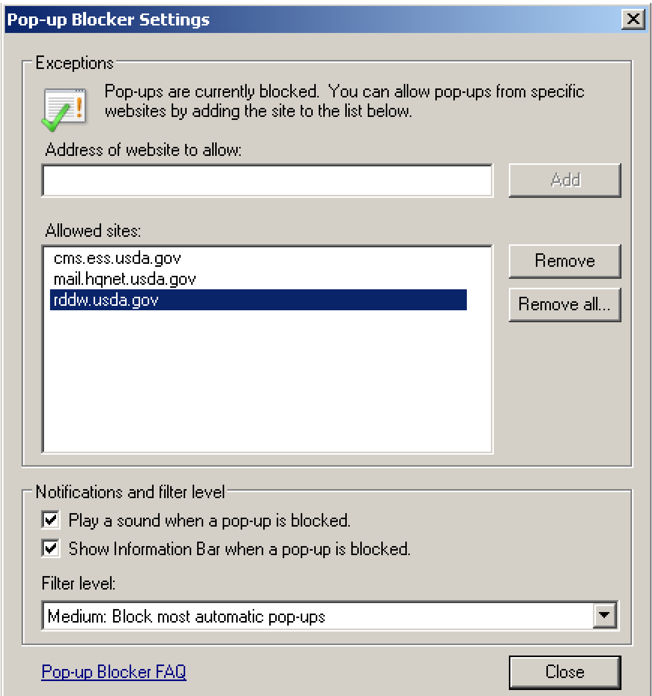


Figure 3: Pop-up Blocker Settings Window

Add the URL of the ECM application (cms.ess.usda.gov) to the list of allowed sites. Internet Explorer does not block pop-up windows from sites on this list. Close the window to return to Internet Explorer.

Internet Explorer Security Settings

Security settings in Internet Explorer must be configured to permit the ECM application to operate properly and to minimize the number of repetitive and unnecessary security warnings.

If a user reports problems with ECM, or if the Internet Explorer displays a security warning in its Information Bar, check to see that the following settings are enabled. (Changing these settings requires administrative access to the user's computer.)

As displayed below, select **Internet Options** from the Internet Explorer **Tools** menu.

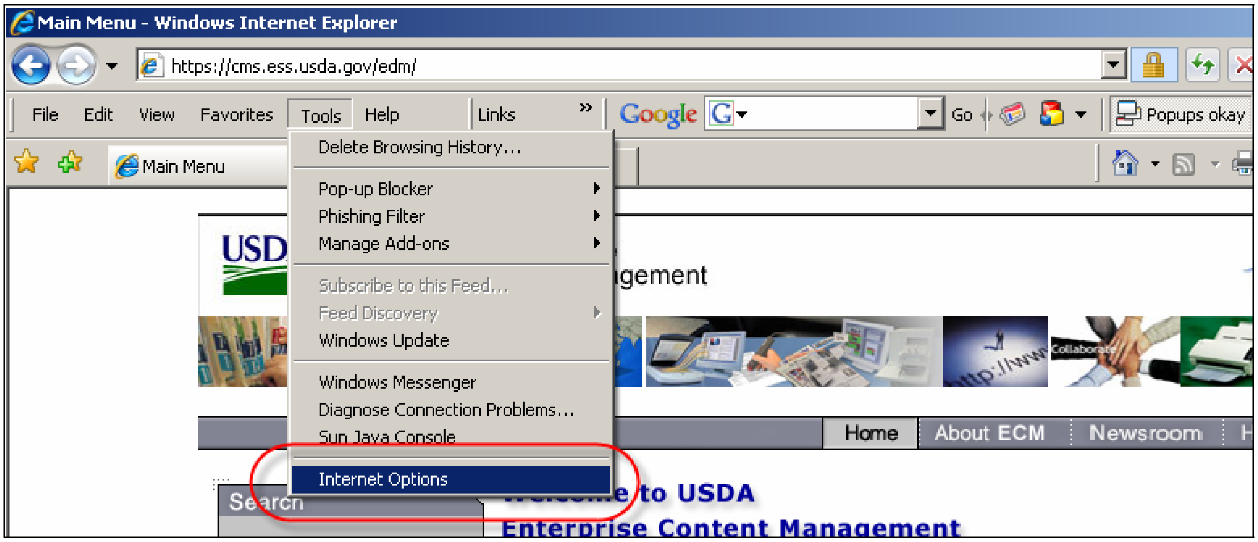


Figure 4: Internet Explorer (Open Internet Options From Tools Menu)

This will open a new **Internet Options** window.

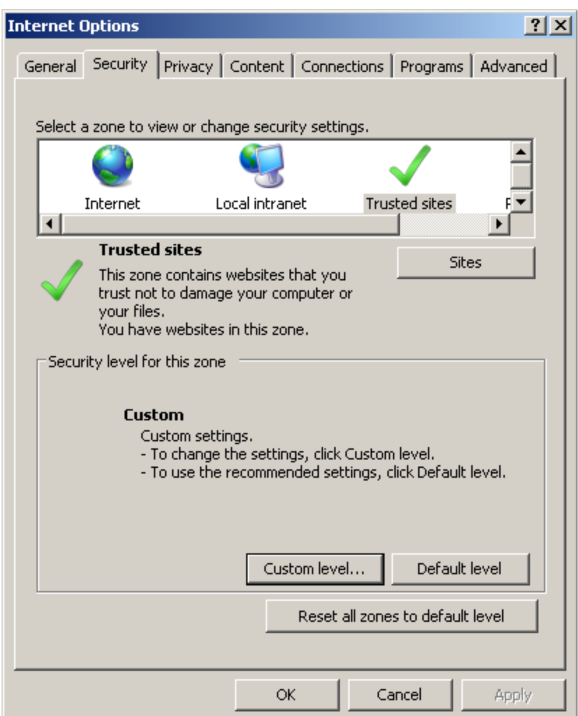


Figure 5: Internet Options (Security Tab; Selecting Trusted Sites Zone)

When the **Internet Options** window is displayed, select the **Security** tab. Note the different security zones. Security settings are maintained separately for each zone by Internet Explorer.

Any custom settings will apply **only** to the zone in which they are defined. ECM should run in the **Trusted sites** zone, and changes should be made to that zone. The changes suggested for ECM may not be appropriate for other zones.

Warning: Do not include sites not known to be trustworthy in your trusted sites list.

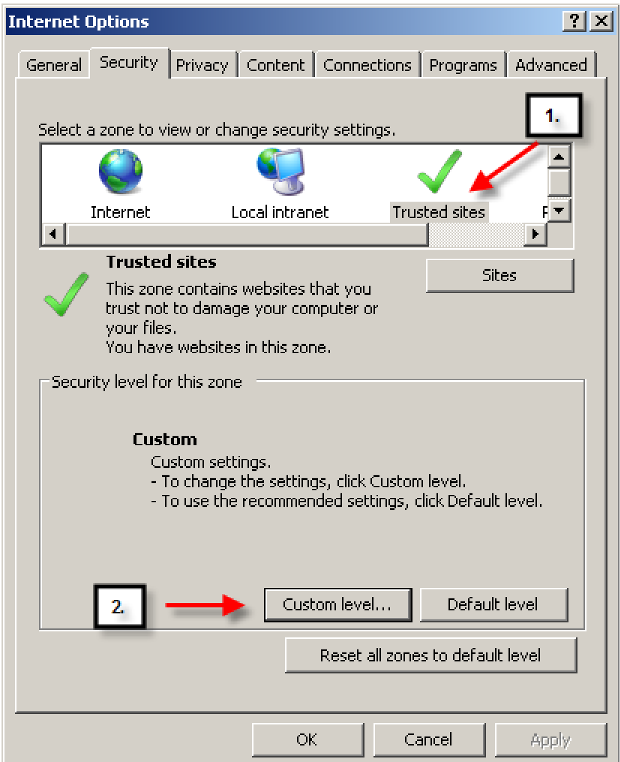


Figure 6: Internet Options Window (Security Tab: Trusted Sites, Custom Level)

We will be making changes only to the **Trusted Sites** Z**one.** Testing indicates this is adequate with Internet Explorer version 7.0. Depending on the version of browser and the security updates installed, additional changes in other zones may be required to limit security warnings.

First, select the **Trusted Sites Zone;** second, click the **Custom level** button as shown above. This will open the Security Settings window.

Disable Display Mixed Content Warning

If this setting is not enabled, the user frequently is warned that the page to be displayed contains secure and non-secure portions. In the Security Settings, scroll to **Display mixed content,** and ensure the **Enable** radio button is selected; click **OK**. Answer **Yes** on the warning asking "Are you sure you want to change the security settings for this zone?"

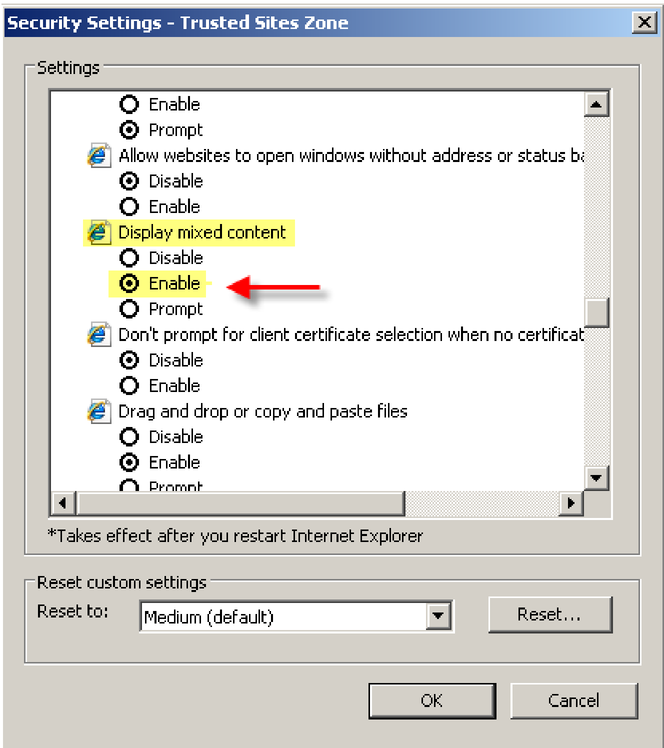


Figure 3

Note: In some versions of Internet Explorer, this change may be required for the Internet Zone in order to limit the security warnings.

Change Security Settings

Three additional security settings must be enabled on the Security Settings in Internet Explorer for the Trusted Sites Zone if ECM is to work properly. They are:

Automatic prompting for file downloads
File download
Initialize and script ActiveX controls not marked as safe for scripting.

The correct settings are displayed in the figures below:

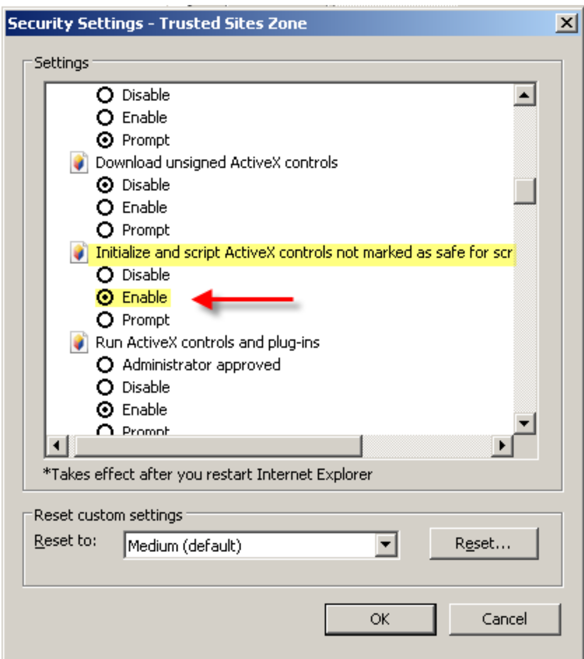


Figure 7: Security Settings (Active X)

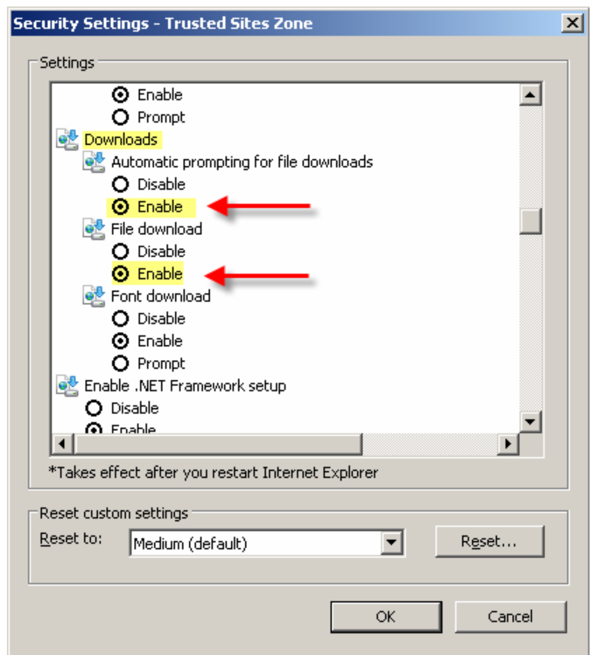


Figure 8: Security Settings: File Download

After these changes are made, save the selections by clicking on the OK button at the bottom of the window. The user is returned to the Internet Options windows. Save the changes by clicking on the OK button at the bottom of the window.

Timing Out of the Application

USDA information technology security regulations require web applications (such as ECM) to close if they are inactive for more than a few minutes. This prevents unauthorized use of the application through an unattended computer.

When a user times out, the user must log in to the application again to resume work.

If the user's work session is inactive and times out before changes are saved, those changes are lost. The message shown below is displayed.

Figure 9: Time Out Message

Another Message that indicates the user has timed out of the application is shown below.

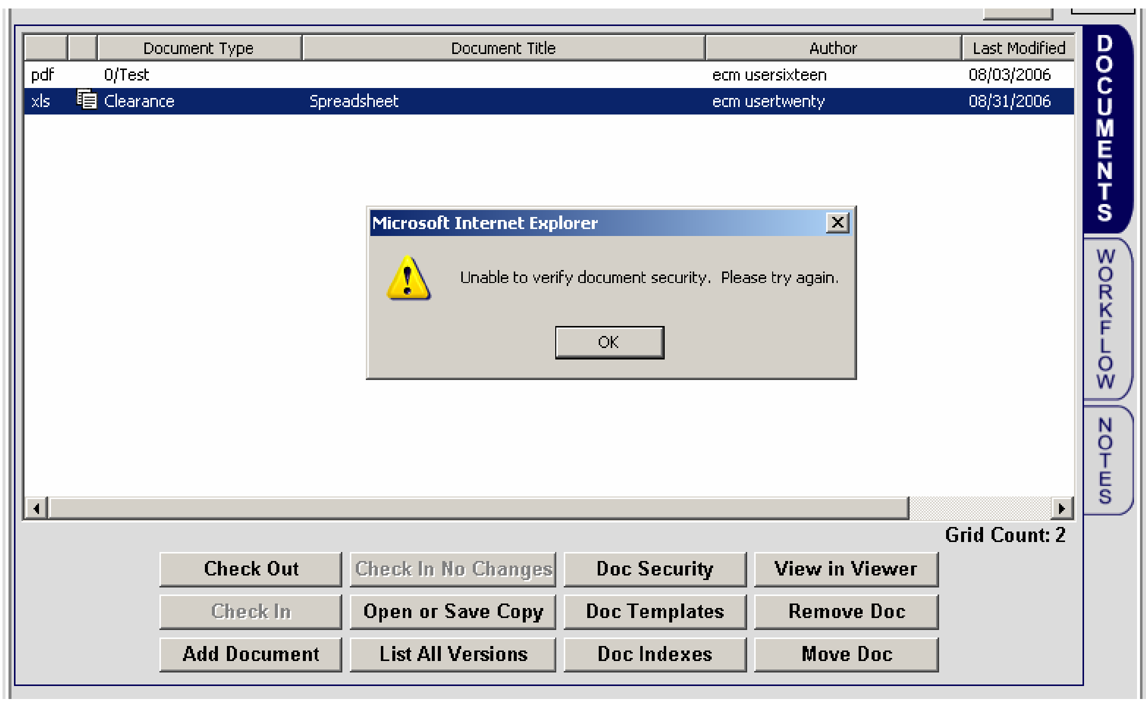


Figure 10: Time Out Message

Messages stating the application is unable to verify security usually indicate that the user has timed out and the user must log in before continuing.

Folder Status (Suspended Folders)

Active Status

The status of a folder (**ACTIVE, SUSPENDED, CLOSED, ARCHIVED**) is indicated at the top center of the main application screen. A folder with uncompleted steps on its workflow is **ACTIVE** unless it has been suspended.

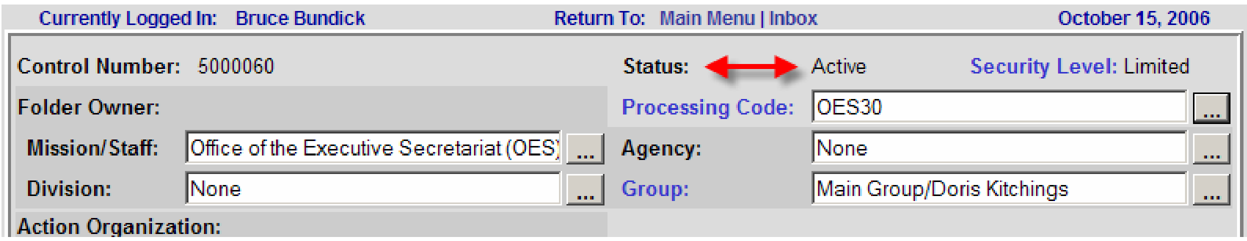


Figure 11: Folder—Active Status

Suspended Status

Sometimes an administrator may wish to temporarily suspend a workflow. The status of a folder may be set to **SUSPENDED** by clicking the <Suspend Workflow> button.

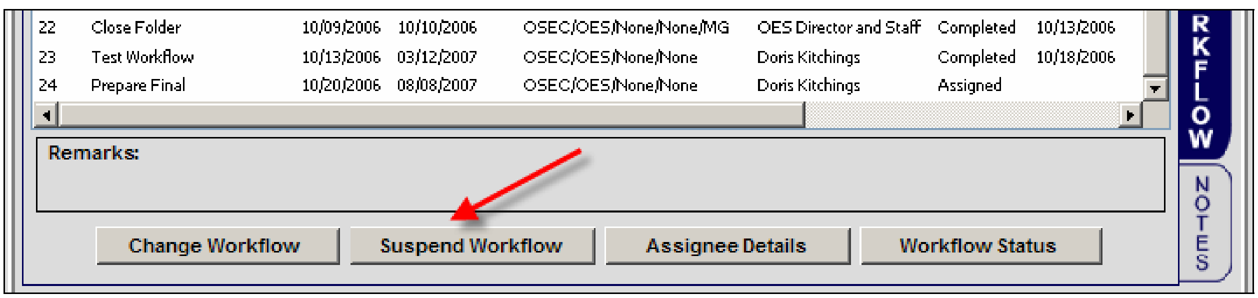


Figure 12: Folder—Suspend Workflow Button

Folder status also may be set to **SUSPENDED** by the ECM application if the user's work session times out due to inactivity while the workflow editor is in use or if the user closes the application from the workflow editor without saving the changes.

A folder with a status of **SUSPENDED** is locked for workflow access, and no workflow steps may be completed. A status of **SUSPENDED** is indicated at the top center of the screen.

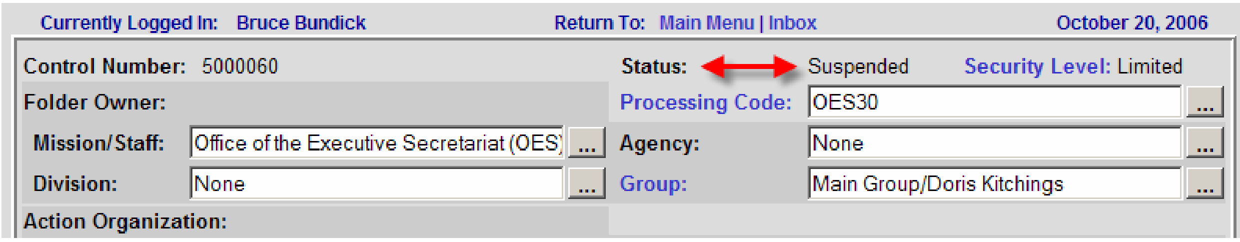


Figure 13: Folder—Suspended Status

As an additional visual cue, the workflow panel on the workflow tab is "grayed out" as displayed in the example below. To change the status of a folder from **SUSPENDED** to **ACTIVE** so that work can be resumed, the user must click the **RESUME WORKFLOW** button as shown below.

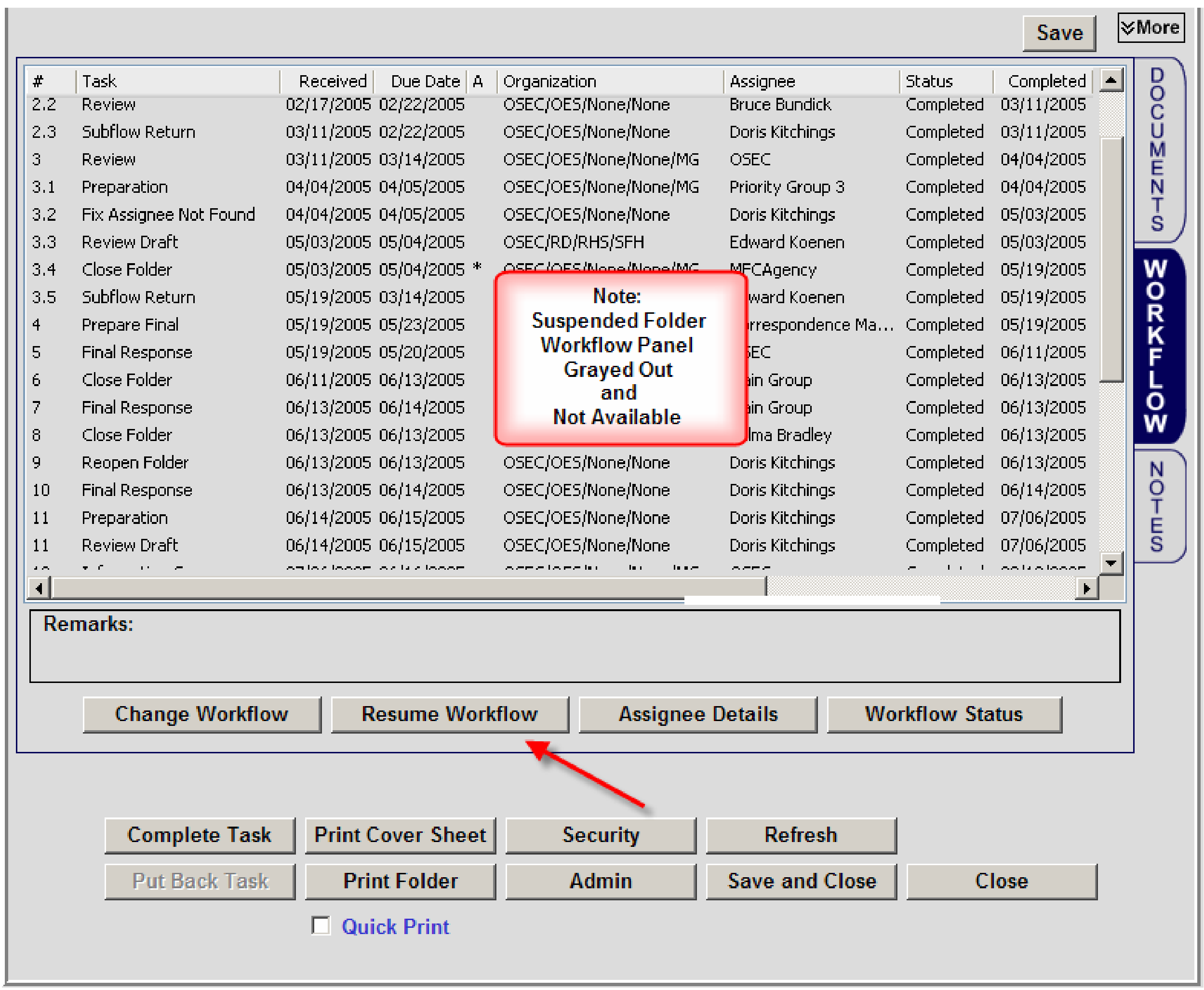


Figure 14: Resume Suspended Workflow

Active, but "Stuck" Folders

For a folder to be visible in a user's inbox, it must have the status **ASSIGNED**, **STARTED**, or **PUT BACK**. Once an assigned folder task has been completed, the folder is no longer visible in the inbox.

At times, a system error can leave the current task with a status of **NOT STARTED** even though all previous non-information tasks have been **COMPLETED**. In such a circumstance, a folder is active, but it does not appear in any user's inbox. A folder owner or administrator can launch the task which will make the next step in the workflow **ASSIGNED** and therefore visible in the user's inbox.

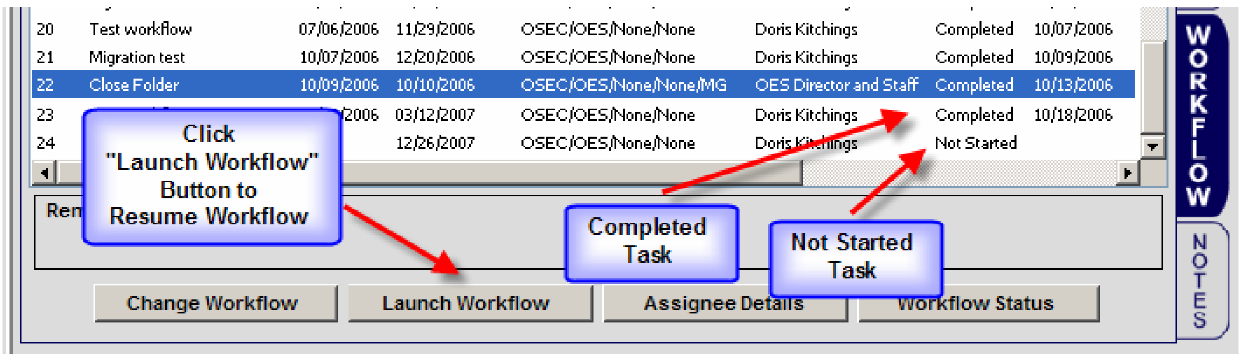


Figure 15: Launching Not Started Tasks

Back Button

The Internet **BACK** button has been disabled in ECM application. DO NOT use the **BACK** button if it is available. The **BACK** button may appear as an icon, a text button, or a icon with text depending upon the configuration of Internet Explorer and its version.

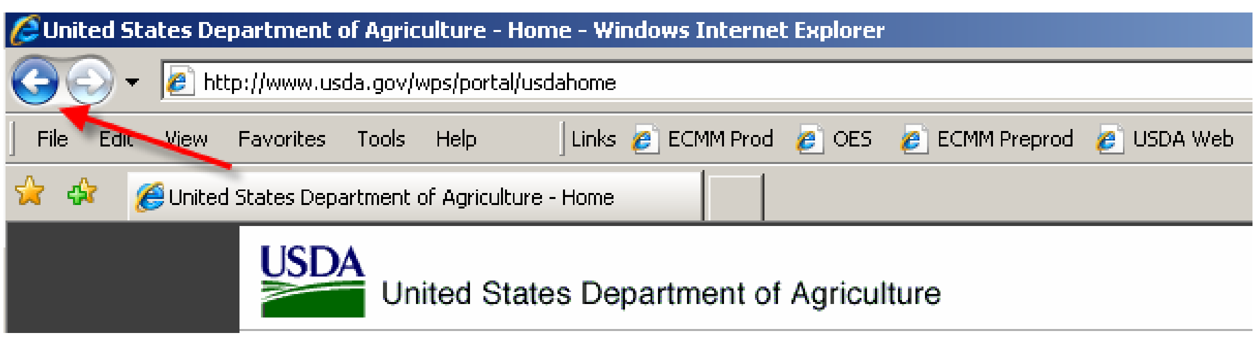


Figure 16: Internet Explorer Version 7.0 Back Button

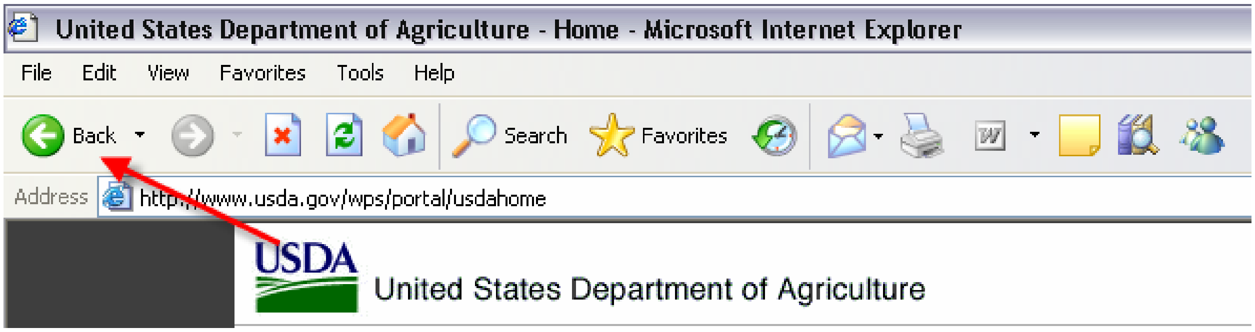


Figure 17: Internet Explorer Version 6.0 Back Button

Navigation within ECM is described in another section of this guide.

Microsoft Office Integration

Two specialized applications are available for use on client computers that facilitate the use of Microsoft Word and Microsoft Outlook with the ECM application.

Microsoft Word Integration

The ECM application allows users to check out, edit, and check in documents directly from Microsoft Word. The ECM application also allows the user to save personal draft copies to the ECM repository without publishing them to the folder. Users do not need to navigate the Windows file system to locate documents to check in to ECM.

Downloading the Word Add-in

The Microsoft Word Add-in can be downloaded by clicking on System Requirements/Download link on the ECM Main Menu as seen below.

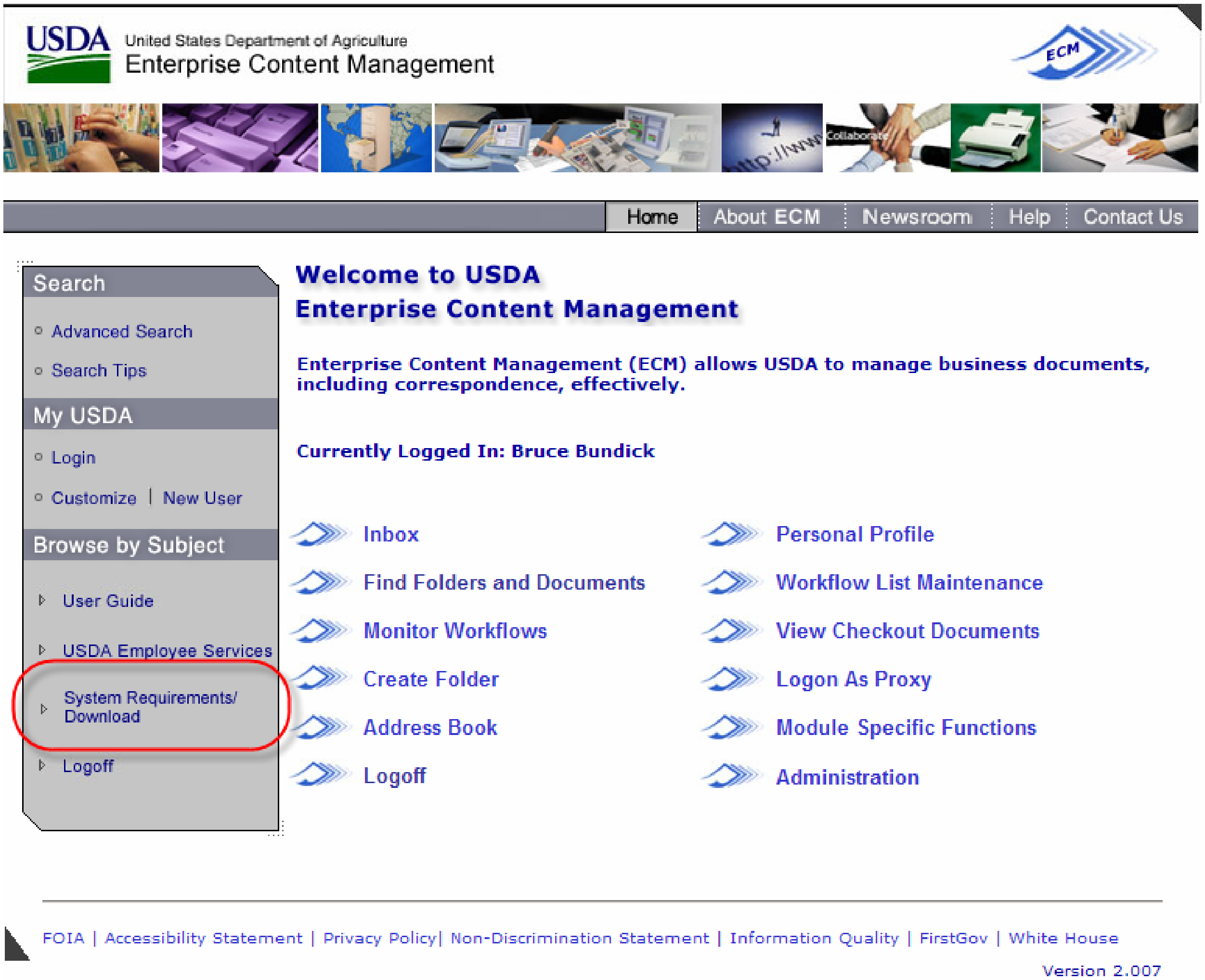


Figure 18: ECM Main Menu - System Requirements/Download

When the menu below is displayed, click on “Instructions for software download for ECM Microsoft word Add-In” and follow the instructions.

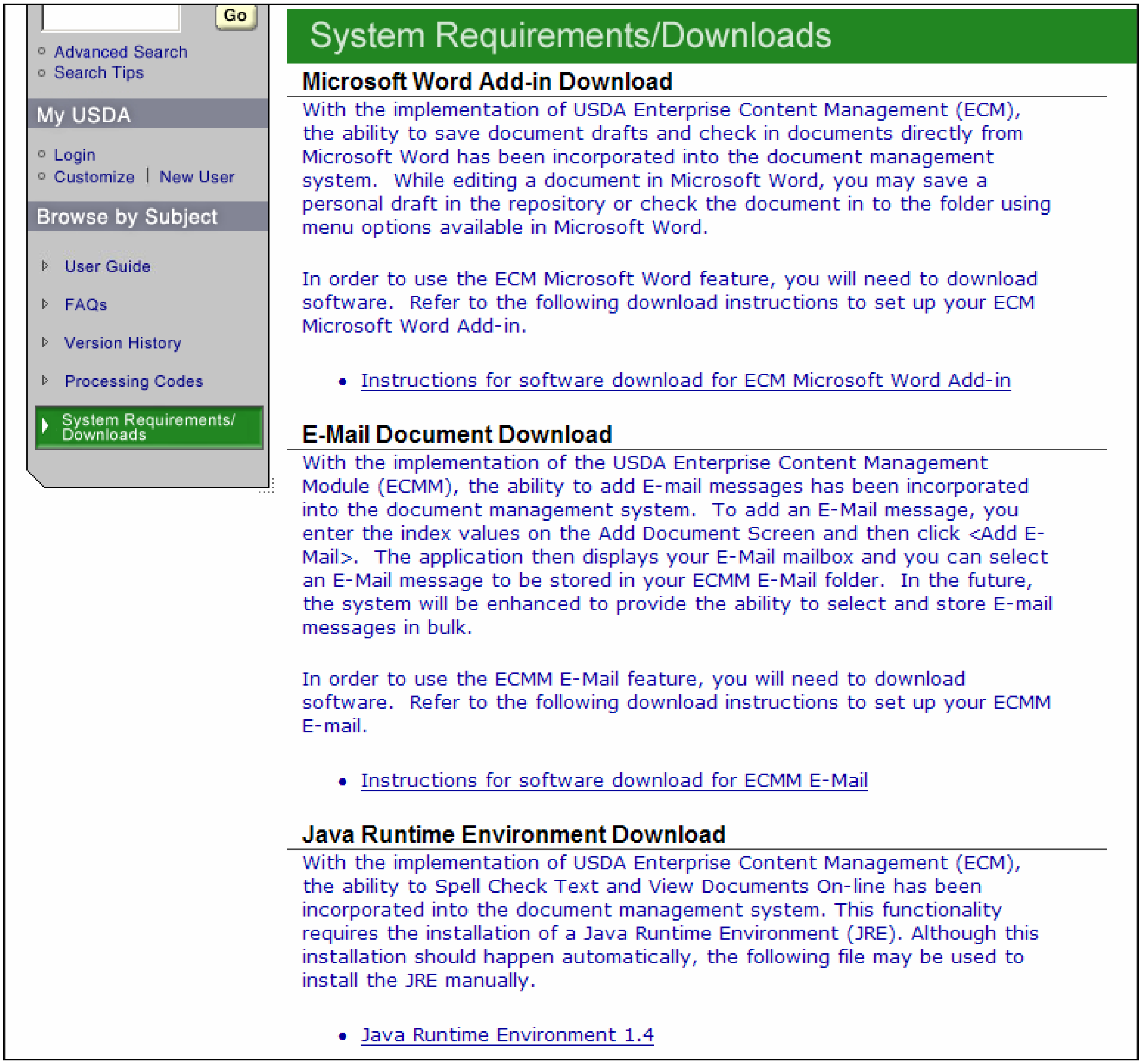


Figure 19: Instructions for software download for ECM Microsoft word add-in

Once the MS Word integration application add-in is installed on a user's workstation, this functionality is available for all modules within the ECM framework.

Microsoft Outlook and Java Downloads

Follow the appropriate links to download the Microsoft Outlook integration application add-in or the Java Runtime Environment as required.

Hints and Suggestions

Proxy Not Working

If a user reports that he or she can no longer see an expected user in the “Logon as Proxy” drop-down list, or if the list is empty, it is likely that the assigned proxy rights have expired or been withdrawn. Proxy rights can be authorized only by the granting user. They cannot be granted by an administrator.

Printing Tips

If a user reports that he or she cannot print a folder, check their default printing setting in their personal profile to determine where the link to the completed print job link has been sent. The user may send the link to a browser window, to his or her ECM inbox, or to the electronic mail account identified on the user’s account. Next, check the default printer settings on the local computer to ensure that the expected printer is the one receiving the job. If no local problem is identified, escalate the call so that ECM system administrators can check the print server.

Workflow Tip (User Unable to Complete Task)

If a user reports that he or she cannot complete a task on a folder, this person is probably not the currently assigned user. First, check to make sure the task is currently assigned to them or to a group of which they are a member. Users often open a folder through a query screen. They may have view access to the folder and be able to open it, but in that case the “Complete Task” button is not available. If the task is currently assigned to a group of which the user is a member, check to ensure the task has not been “Started” on another member of the group.

2. Navigating ECM

Application Logon

To use ECM, the user enters the appropriate URL, http://cms.ess.usda.gov/edm, for the production Enterprise Content Management system. As is the case with many USDA corporate applications, the user's log in request is redirected to the eAuthentication application to log in. The e-Authentication logon screen is shown below. If the log in is successful, the user is returned to the ECM application Main Menu.

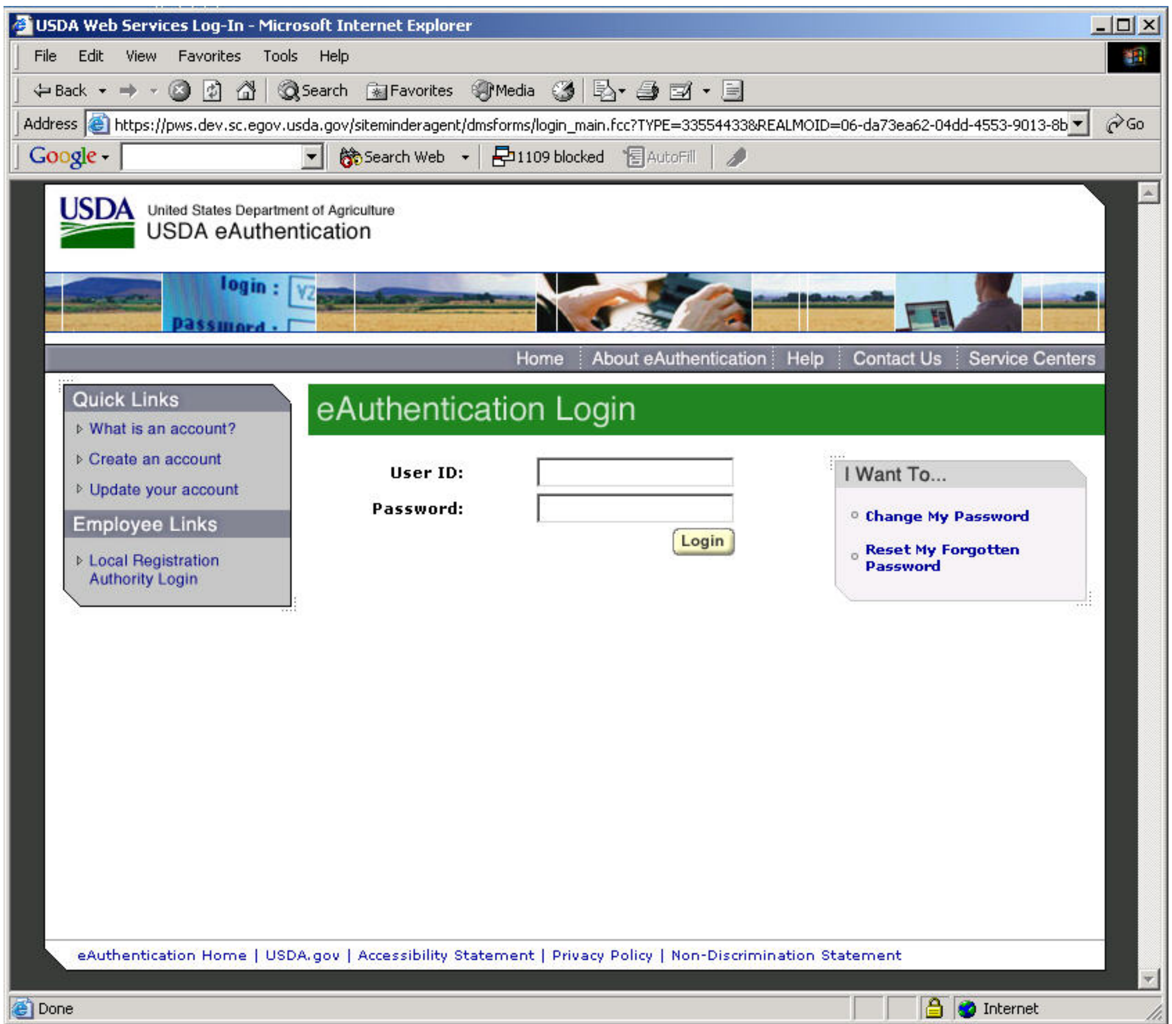


Figure 20: eAuthentication Log In Screen

Password changes or changes to other user account information are managed through the e-Authentication application, not through the ECM application.

Application Access

Unauthorized Access

Users must have a valid eAuthentication account and be an active authorized user of the ECM application. To access the Enterprise Content Management application, the user must have an active account created by an ECM Security Officer, Application Administrator, Module Administrator, or Agency Group Administrator. If a user attempts to access the application but does not have an established ECM account, the Unauthorized Access message shown below is displayed.

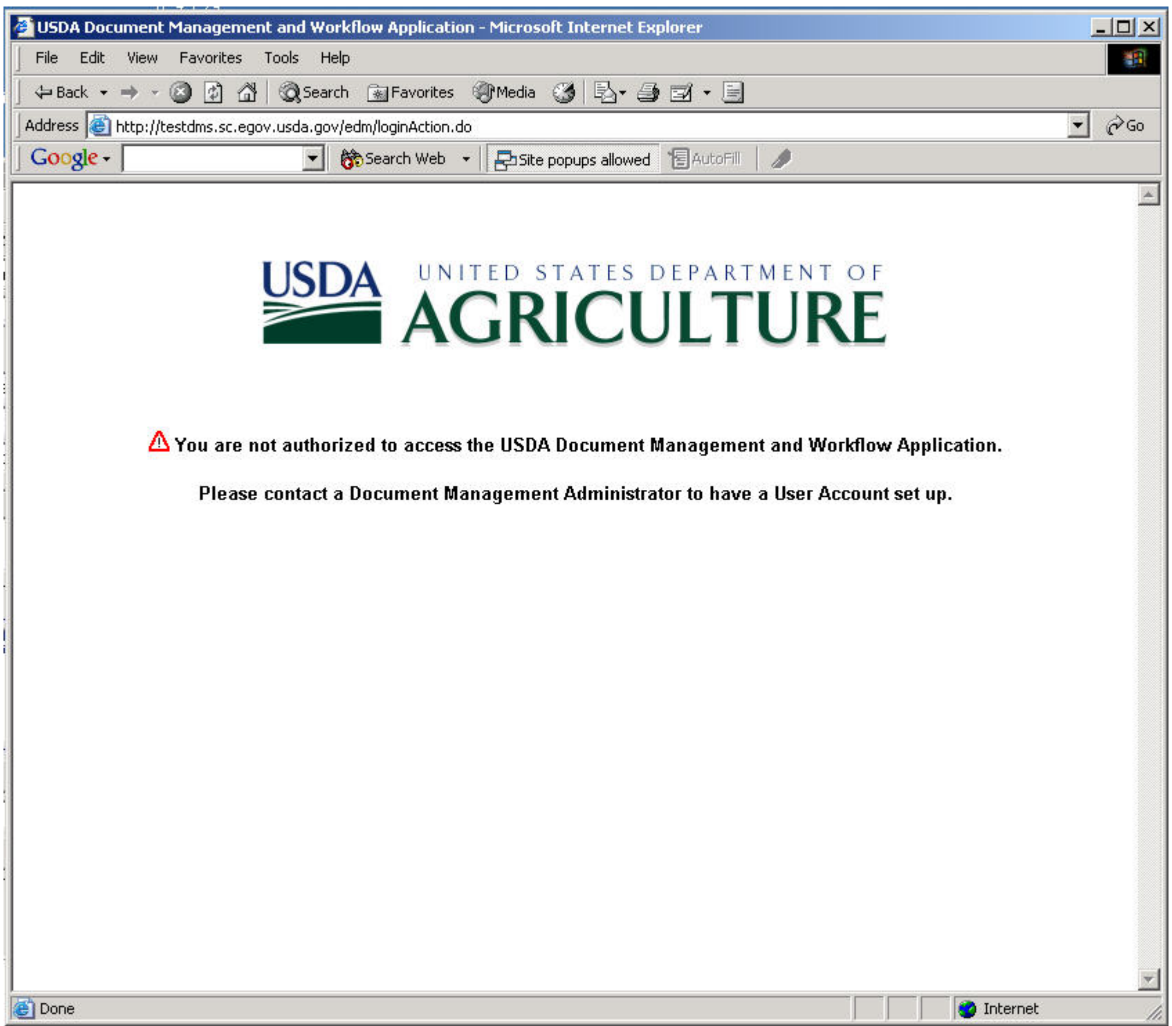


Figure 21: Unauthorized Access Message

Authorized Access/Main Menu

After successfully logging on through eAuthentication, the Enterprise Content Management application main menu is displayed as shown below.

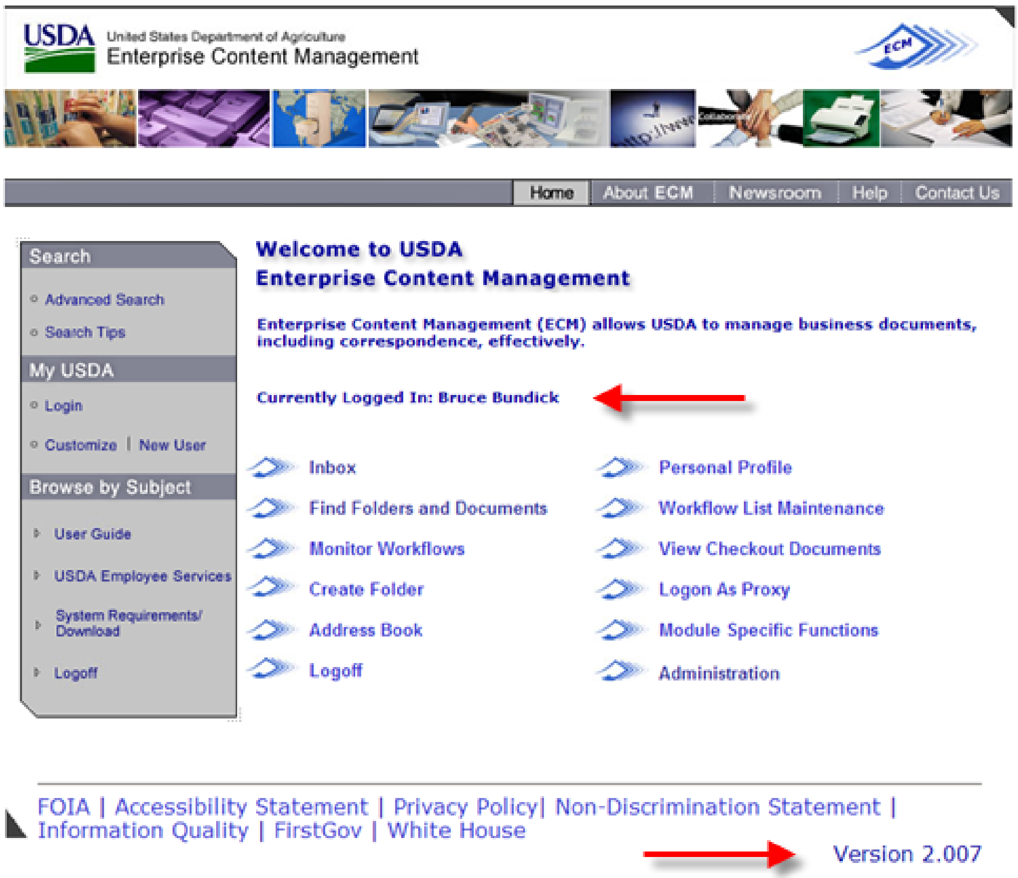


Figure 22: Enterprise Content Management Main Menu

Note that the main menu page displays the identity of the current user and the current version of the ECM application. Depending upon the individual's privileges and role in ECM, all of the menu options may not be displayed and available.

The links on the main menu allow an authorized user to access his or her ECM inbox, query for folders or documents, create a new folder, or perform various administrative functions.

Logon As Proxy

A properly designated user may perform work on the system on behalf of another user. To exercise a proxy, the assigned user must have previously designated the user as someone authorized to perform work on his or her behalf. Granting proxy rights to other users is one of many options in the Personal Profile section of the ECM application.

To log on as a proxy for another person, the user clicks the Logon as Proxy selection on the Main Menu shown highlighted below.

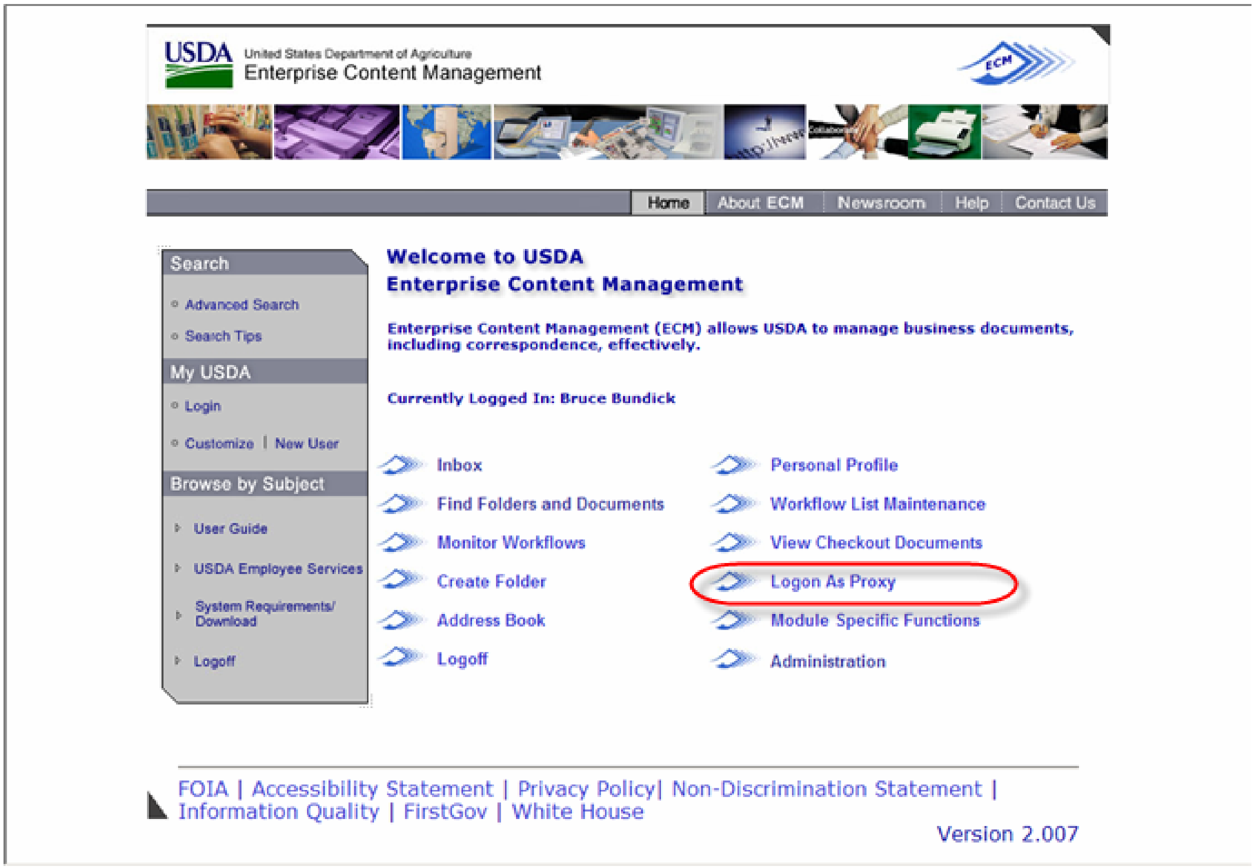


Figure 23: Logon As Proxy Menu Item

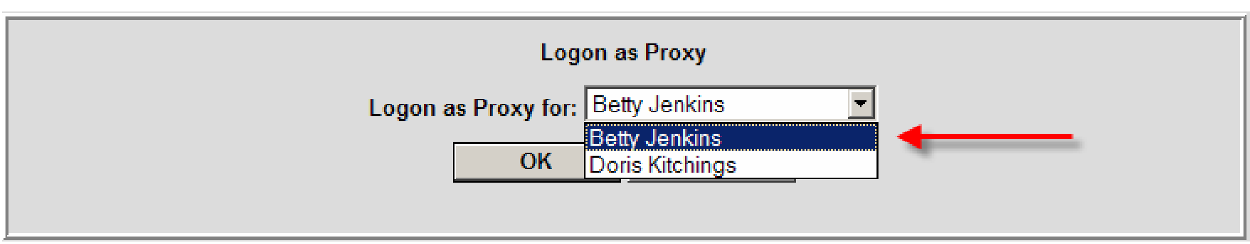


Figure 24: Review Available Proxies

The "Logon as Proxy for" field has a drop-down list that displays all ECM users who have authorized this user to act as their proxy. Use the drop-down menu to display the available users and select the appropriate user.

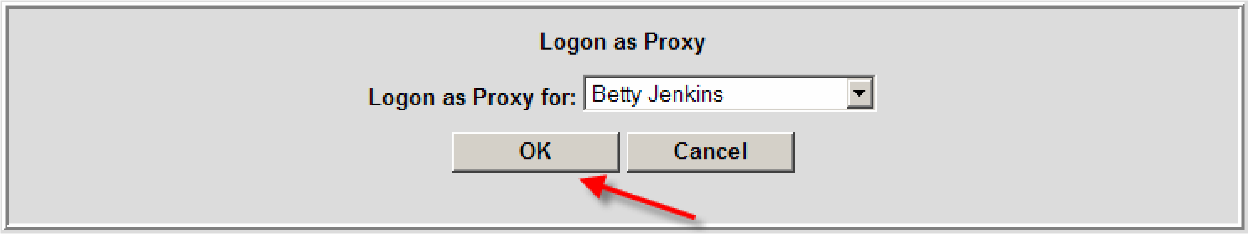


Figure 25: Logon as Proxy

Click the **OK** button to log in as a proxy for the named user.

When logged on as a proxy for another user (in this case Betty Jenkins) the active user (Bruce Bundick) will see Betty Jenkins' inbox and workflow assignments. While acting as a proxy, the active user temporarily inherits and exercises Betty Jenkins' privileges and responsibilities, except that proxy rights do not include administrative privileges. The active user does not see a "combined" inbox (Betty Jenkins and Bruce Bundick)—just the inbox of the proxied user (Jenkins).

Note that in the figure below the current user is identified as "Bruce Bundick as proxy for Betty Jenkins." To stop acting as a proxy for Betty Jenkins, the user Bruce Bundick selects the Logoff as Proxy item on the Main Menu.

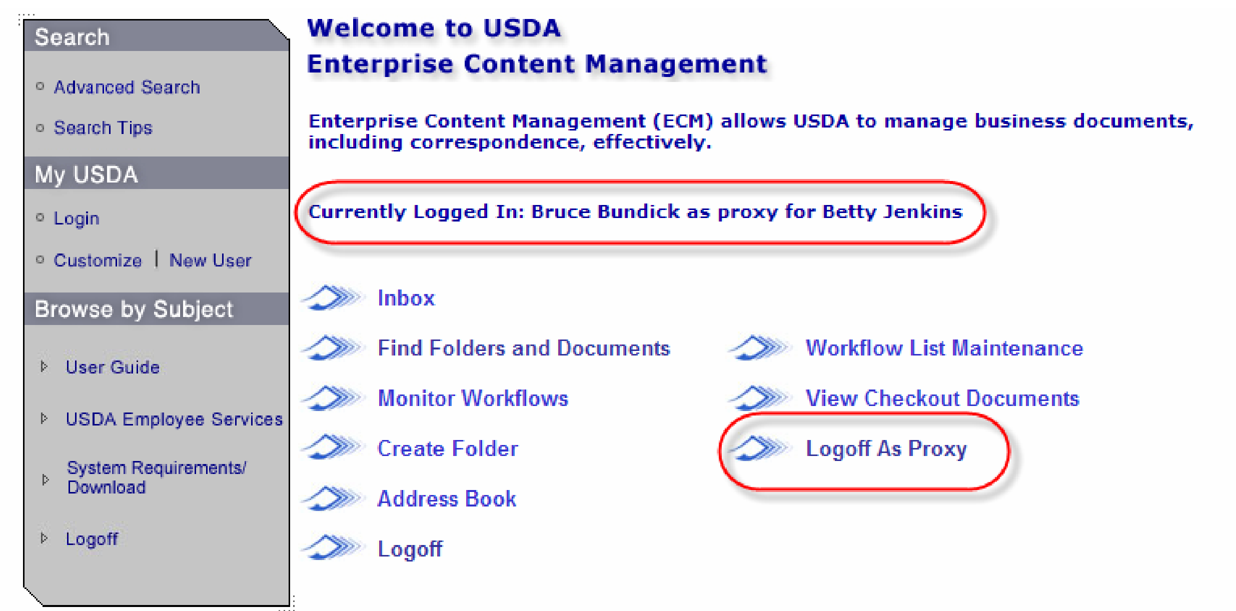


Figure 26: Logoff As Proxy

The “Logon as Proxy” screen is again displayed. The user selects the “No Proxy” item from the drop-down list and clicks the **OK** button. The user is returned to his or her own login identity with access to his or her own inbox, folders, and privileges.

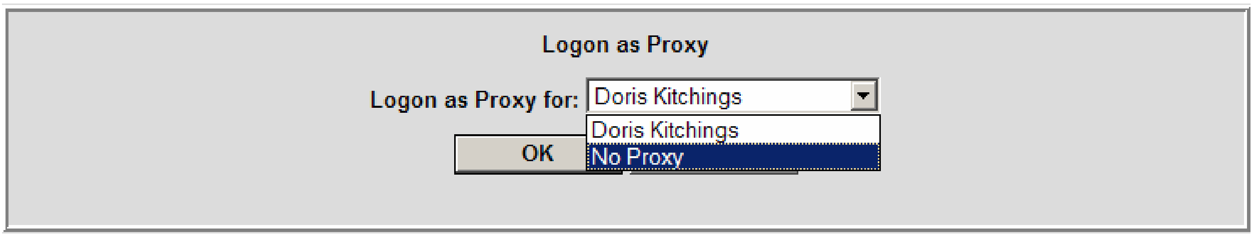


Figure 27: Logoff as Proxy

Note: The proxy function is handled by the ECM application, not the e-Authentication system.

Application Logoff

To close the application, the user clicks the Logoff option on the main menu as seen below.

Figure 28: Logoff From the Main Menu

The confirmation screen in the figure below is displayed.

Figure 29: Logoff Confirmation Screen

The screen includes a link that allows the user to return to the Logon screen for the application.

Navigating Though the Application

Return To: Main Menu | Inbox

Close

Save And Close

Cancel

Update And Return

Main Menu

Sub-Menus

Return To: Main Menu | Inbox

Navigation is easy within ECM. From the top of most screens, the user can go directly to the MAIN MENU or the INBOX by clicking on the desired location next to "Return To:" at the center of the page, as shown below.

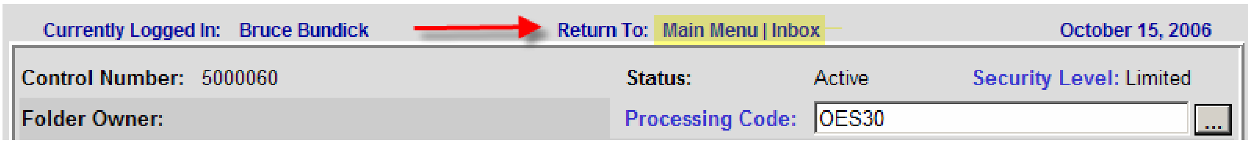


Figure 30: Return to: Main Menu | Inbox

If a user makes changes to a folder or task and attempts to return to the Main Menu or Inbox before saving changes, the warning message shown below will be displayed. The user can click **OK** to discard the changes and continue to exit, or click **CANCEL** to return on the current task/folder with the opportunity to save the changes.

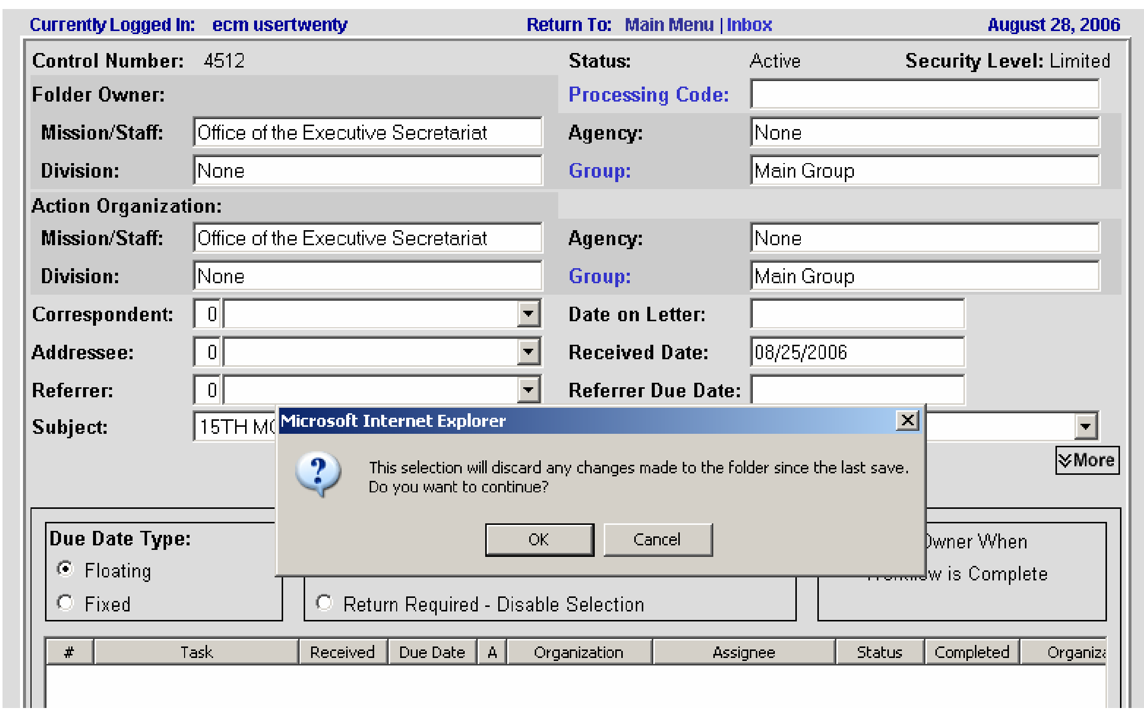


Figure 31: Folder Navigation – Return to: Main Menu | Inbox – Save Changes Warning

Close

On ECM screens such as the “Workflow Inbox” below, the user may leave the screen simply by clicking the **CLOSE** button. This action will return the user to the previous screen.

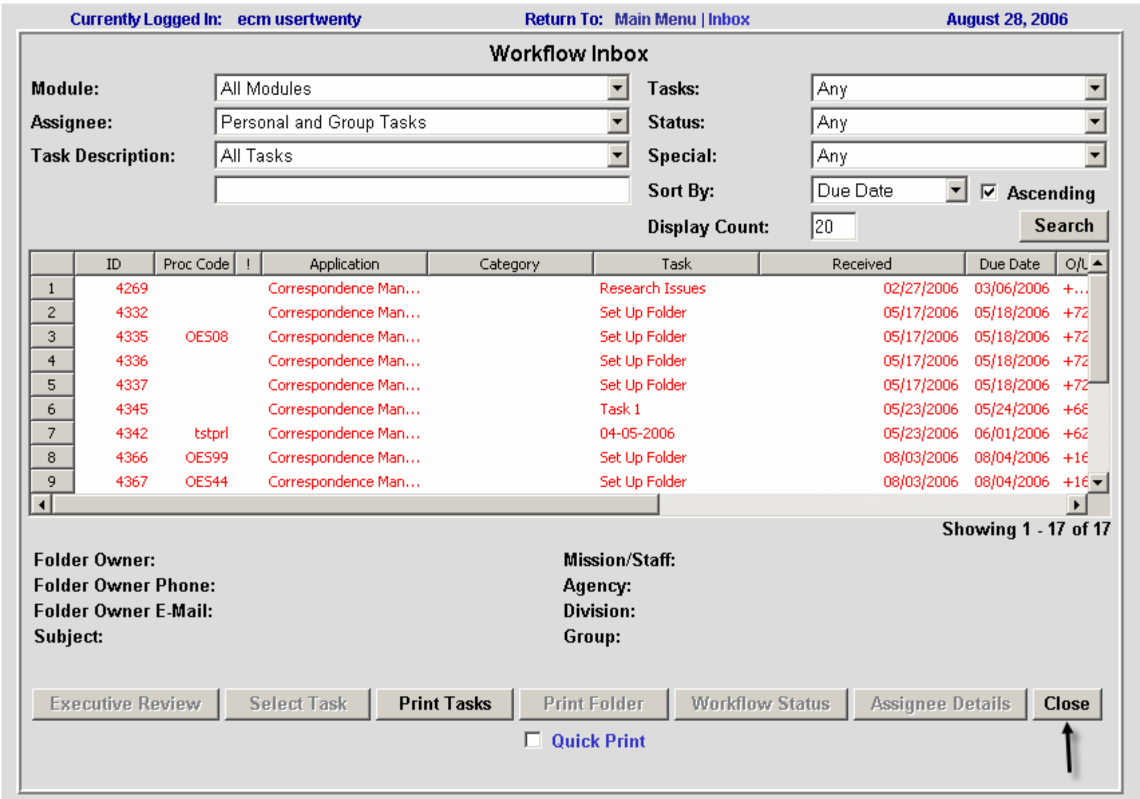


Figure 32: Workflow Inbox - Close

When the user selects a task to work on, or opens a folder, the user is often making changes to information in the folder. Since those changes are not transmitted to the application servers until the page is saved, closing a folder can cause information to be lost.

If the user makes changes and then attempts to ‘Close’ a folder without saving the changes, the message shown below is displayed. The user can click **OK** and close the folder without saving the changes, or click **CANCEL**, which terminates the close folder action and permits the user to save changes before closing.

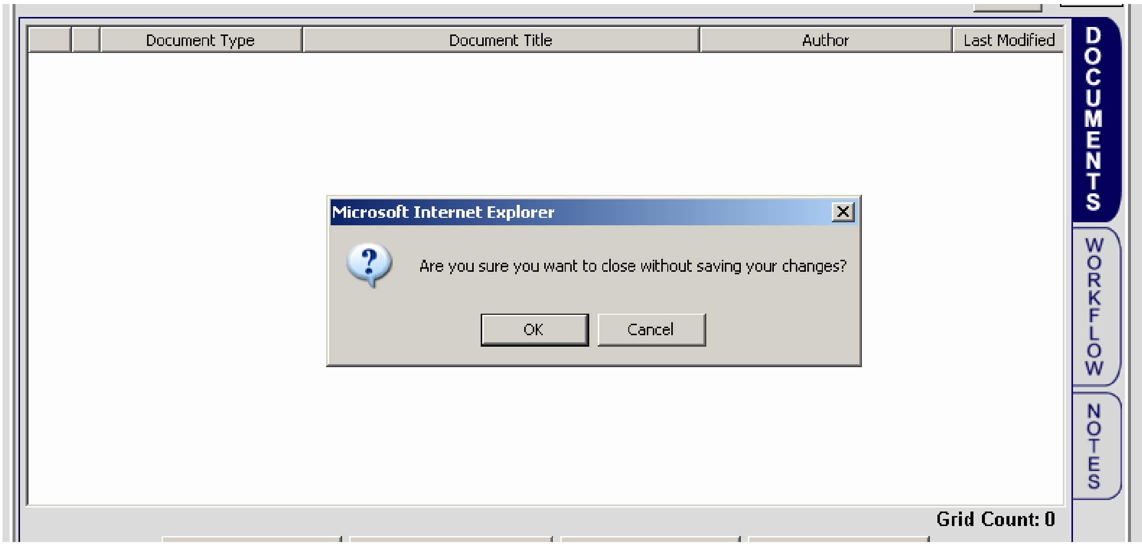


Figure 5: ECM Folder–Attempting to Close Without Saving Changes

Save and Close

When a folder or task has been opened, the folder can be **CLOSED** if there were no changes made or if those changes should be abandoned. The folder can be **SAVED** if changes have been made and the user intends to continue to work on the folder. If work on the folder is complete, the user can save changes and exit the folder with a single action, clicking the **SAVE AND CLOSE** button. After the changes are saved, the user will be returned to the screen from which the folder or task was originally opened—usually the Inbox or the Find Folders and Documents query screen.

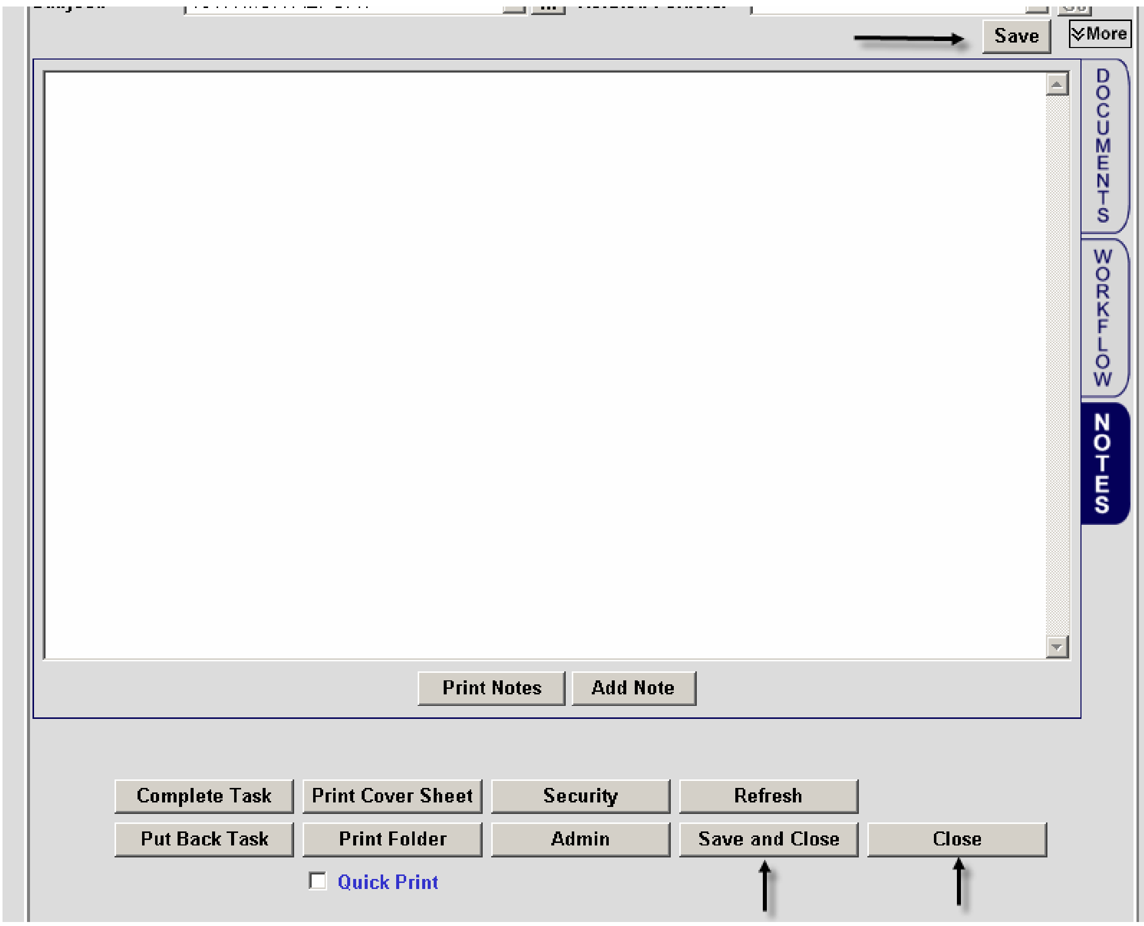


Figure 33: Workflow Inbox—Save and Close

Cancel

In ECM, **CANCEL** stops the current action and returns the user to the previous task. In the examples above, **CANCEL** was used to stop an action, such as leaving a folder and returning to the Main Menu. In that case, the user was returned to the previous action. The **CANCEL** option shown below stops the query and returns the user to the Main Menu or other parent screen.

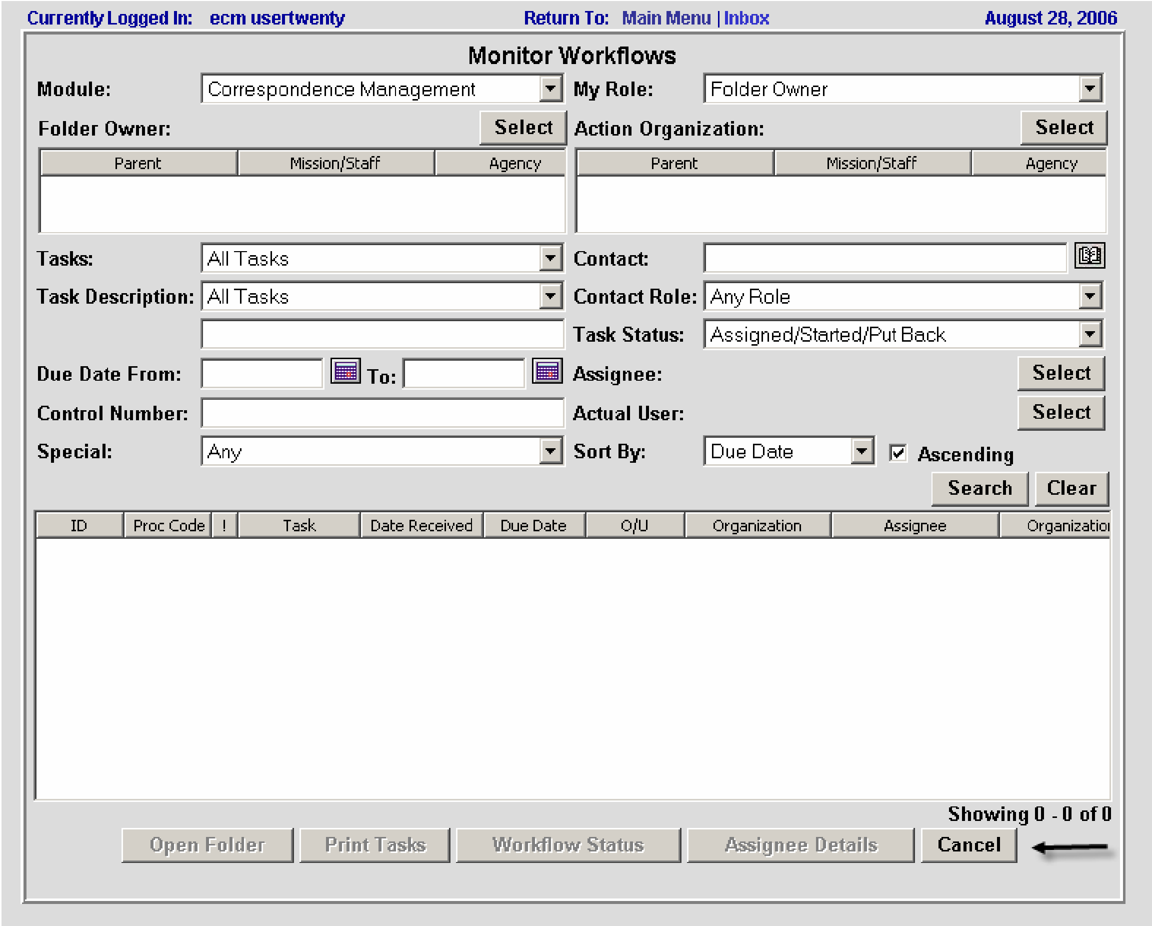


Figure 34: Cancel

Update and Return

The Workflow Editor is accessed by clicking **CHANGE WORKFLOW** button on the Workflow Tab on a folder. After changes have been made to the workflow, the two options are **CANCEL** and **UPDATE AND RETURN** as shown below.

CANCEL discards the changes made in the workflow editor and returns the user to the Workflow Tab of the folder. **UPDATE AND RETURN** saves the changes made in the workflow editor and returns the user to the Workflow Tab of the folder.

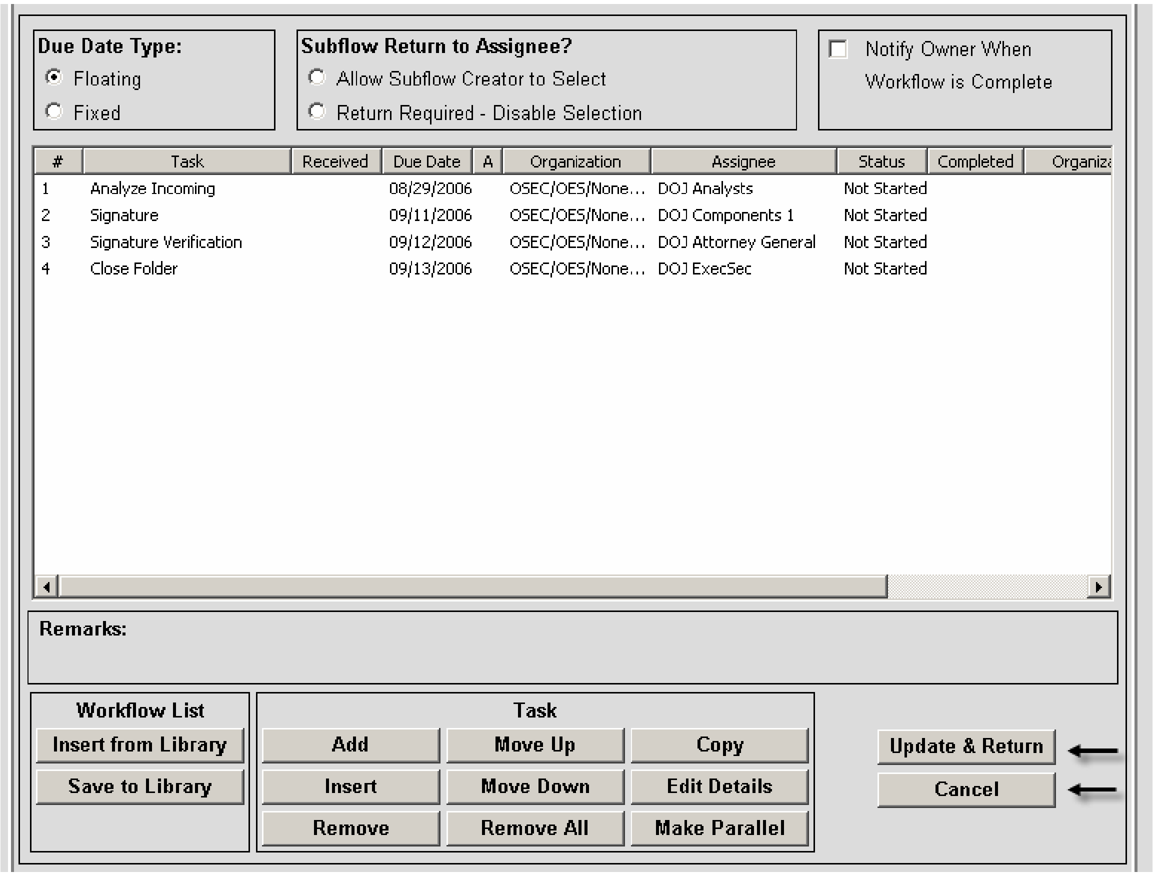


Figure 35: Workflow Editor–Update & Return and Cancel

Main Menu

⇒ The initial ECM screen is the Main Menu, which provides personalized access to ECM and its features. Links around the margin of the page provide access to application information (such as "About ECM," "Newsroom," and "Help" as well as links to external resources such as USDA's Web Search and your "My USDA" account. The "Browse by Subject" links provide access to technical information for ECM users.

⇒ Your current logon name will always be displayed on the Welcome Screen and all other ECM screens.

⇒ The version number, displayed at the lower right corner of the page, is updated every time there is a change to the ECM application.

Your screen should look similar to the image below:

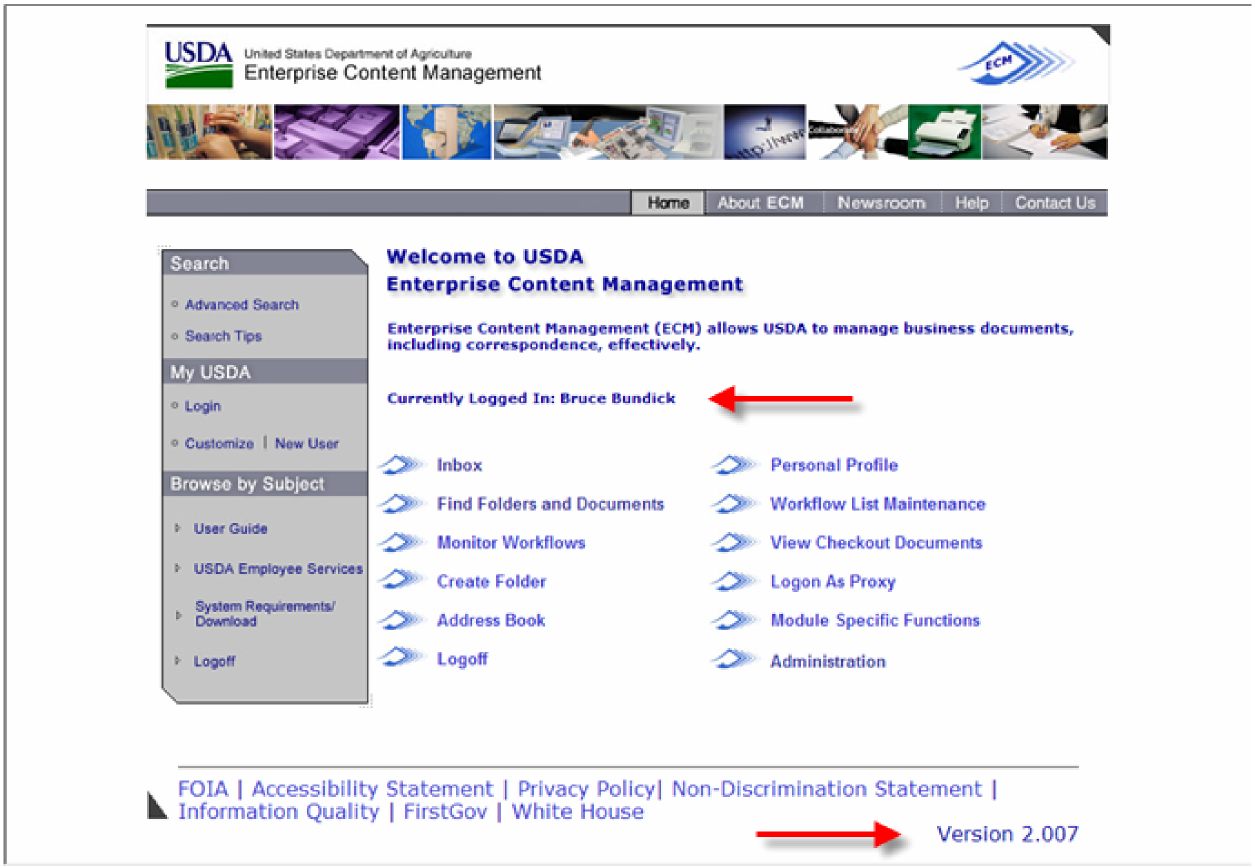


Figure 36: ECM Main Menu

Sub-Menus

For users with the appropriate authorizations, the Main Menu displays two options, “Module Specific Functions” and “Administration” that take the user to separate sub-menus. The “Module Specific Functions” sub-menu is displayed below.

A user choosing the “Close” option from either of these menus is returned to the Main Menu.

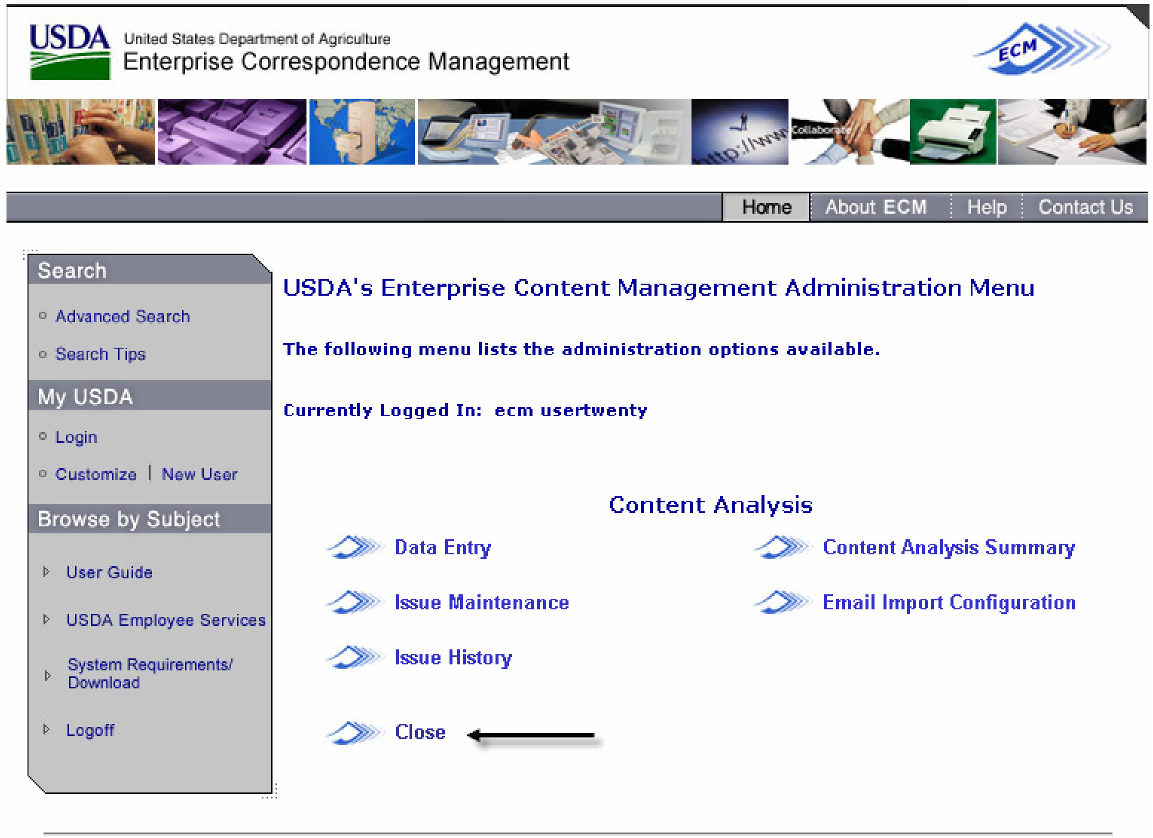


Figure 37: Module Specific Functions Sub-Menu of the Main Menu

Administrator Sub-Menu

To access the Administrator Sub-Menu, select the Administration link on the Main Menu.

Figure 38: Administration Link on ECM Main Menu

If you are designated as an administrator, the Administration link will appear in the lower right corner of your main menu. When you click on Administration, you will be presented with the Administration Menu. Only the items that you are authorized to manage are displayed.

The Sub-Menu is dynamic, and only those items for which a particular user has authorized access will appear on the page. The following Administration Menu is that of a user with Module Administrator privileges. Note that the two items restricted to Application Administrator, <Add/Change U.S. Holidays> and <Add/Change Mission/Staff, Agency, Division> are not displayed.

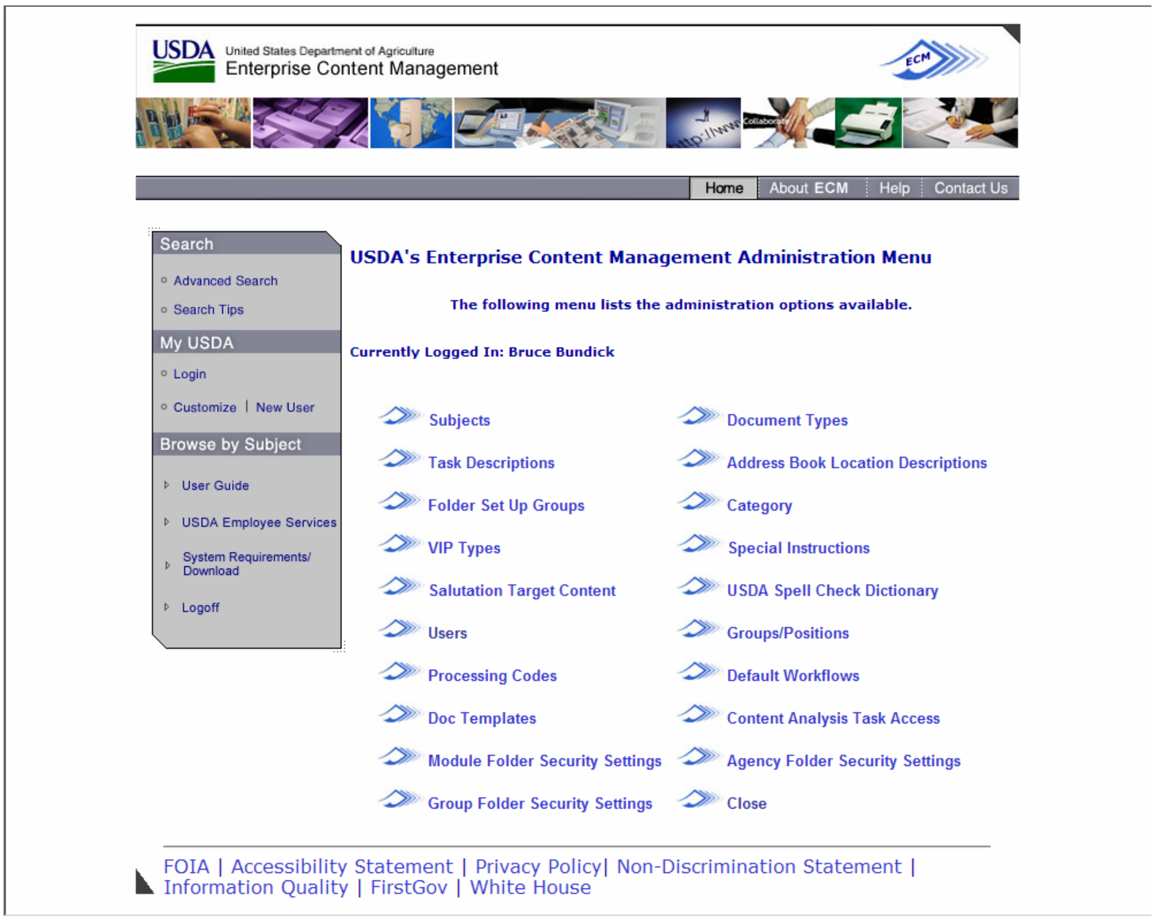


Figure 39: ECM Administration Menu (With Module Administrator Privileges)

Administration Menu Sub-Menu Items

The following table briefly describes the various Sub-Menu items on the ECM administration menu. Each description identifies the administrators with access to the function described.

Link	Description
Add/Change U.S. Holidays	An administrative console for defining official Federal holidays within the application. The holidays are excluded from business days when task due dates are calculated. *Application Administrators only.*
Add/Change Mission/Staff, Agency, Division	An administrative console for defining the three upper levels of the USDA business hierarchy: Mission Areas/Staff Offices, Agencies, and Divisions. Shared across application. *Application Administrators only.*
Subjects	A list of subjects that can be added to the folder. There is a default list for each module. Groups can own their own lists which can include some or all items from the module master list. Groups use the values of the first parent group with its own list. If no parent group has its own list, the group uses the default module list. (LOV item.) *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*
Document Types	A list of document types that can be added to the folder. There is a default list for each module. Groups can own their own lists, which can include some or all items from the module master list. Groups use the values of the first parent group with its own list. If no parent group has its own list, the group uses the default module list. (LOV item.) *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*

Task Descriptions	A list of standard workflow tasks that can be added to the workflow in a folder. There is a default list for each module. Groups can own their own lists which can include some or all items from the module master list. Groups use the values of the first parent group with its own list. If no parent group has its own list, the group uses the default module list. (LOV item.) *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*
Address Book Location Descriptions	An administrative console that is used to define address book locations by module. Currently there are two: Home Address and Work Address. *Application and Module Administrators only.*
Folder Set Up Groups	An administrative console used to define folder Set Up Groups, the groups to which the Kofax scanning and pre-processing application sends folders for initial action. Shared across the application. *Application and Module Administrators only.*
Category	An administrative console to manage categories, a special data element of the General Use Module used to describe types of folders. In the General Use Module, certain features (such as default workflow) can be linked to this data element. The categories are shared across the module. *Application and Module Administrators only.*
VIP Types	A correspondence module data element describing categories of "very important persons" (VIP). The list is shared across the module. *Application and Module Administrators only.*
Special Instructions	A correspondence module data element describing special instructions. The list is shared across the module. *Application and Module Administrators only.*
Salutation Target Content	An administrative console to define key words used by application to locate the salutation in correspondence from within OCR text. This feature is used in ECMM Kofax pre-processing to prepare an automated synopsis. Shared across the application. *Application and Module Administrators only.*

USDA Spell Check Dictionary	An administrative console that is used to maintain the application spell check dictionary. Shared across the application. *Application and Module Administrators only.*
Users	An administrative console used to enroll users in the application, make them active or inactive, place them in groups, and grant various privileges. *All Administrators and Security Officer. Each level of Administrator has different privileges.*
Groups/Positions	An administrative console used to create and manage groups and positions, and to add users to groups. *All Administrators and Security Officer. Each level of Administrator has different privileges.*
Processing Codes	An administrative console for creating and managing processing codes for Mission Areas/Offices, Agencies, Divisions, or groups that can be tied to default workflows. *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*
Default Workflow	The default workflow link allows administrators to tie default workflows to processing codes for a Mission Area, Office, Agency, Division, or group. *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*
Doc Templates	An administrative console that allows administrators to manage (add, delete, edit) document templates in the template libraries. *All Administrators (Agency Group Administrators and Group Administrators if they have administrative privileges for the target group or for a parent of that group.)*
Content Analysis Task Access	An administrative console to grant users permission to access tasks within the Content Analysis module. *Application and Module Administrators only.*

Module Folder Security Settings	An administrative console for defining the available range of module security settings and the default settings within that range. *Application and Module Administrators only*.
Agency Folder Security Settings	An administrative console for defining the available range of agency security settings and the default settings within that range. *Module Administrators and Agency Group Administrators and Group Administrators (if they have administrative privileges for the target group or for a parent of that group.)*
Group Folder Security Settings	An administrative console for defining the available range of group security settings and the default settings within that range. *Module Administrators and Agency Group Administrators and Group Administrators (if they have administrative privileges for the target group or for a parent of that group.)*
Close	Returns the user to the parent menu, in this case the Main Menu.

Table 1: Administrator Sub-Menu Items

3. Managing Groups and Users

Selecting Groups and Users: An Overview

USDA Organizational Hierarchy

The U.S. Department of Agriculture has a hierarchical organizational structure. The top four levels of the USDA hierarchy are represented in the ECM application. It is left to each organization to design and implement the group structure other than these four administrative levels.

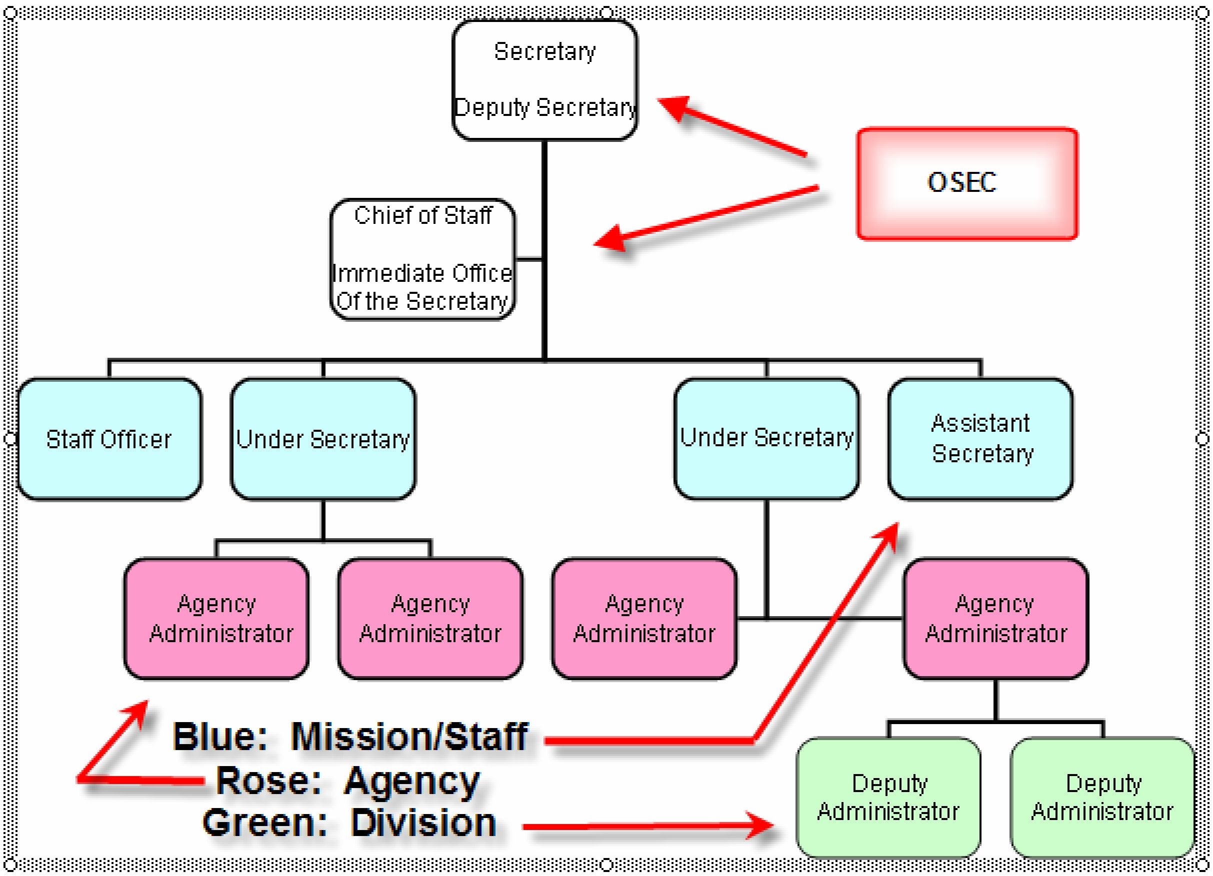


Figure 40: USDA Organization Hierarchy

OSEC Level: At USDA and in ECM, the top organizational level is the Office of the Secretary of Agriculture (OSEC). The Secretary of Agriculture, the Deputy Secretary of Agriculture, the Chief of Staff, the Deputy Chiefs of Staff, and various other senior officials are part of OSEC.

Mission/Staff Level: The next organizational level is known in ECM as the Mission/Staff level. At USDA this level is often called the “subcabinet” level. This level includes: the Under

Secretaries, who are responsible for a "mission area" or group of related agencies (examples: Under Secretary for Rural Development; Under Secretary for Food Safety); Assistant Secretaries who are responsible for an administrative office (examples: Assistant Secretary for Congressional Relations; Assistant Secretary for Administration); and Staff Officers who are responsible for a management of a Staff Office (examples: General Counsel; Chief Information Officer). An organization chart displaying the "subcabinet" level is available on USDA's website. Follow the links to "About USDA" and "USDA Organization Chart." (The box labeled Executive Services includes the Office of Budget and Program Analysis, the Office of the Chief Economist, and the Office of the Executive Secretariat.)

Agency Level: The third organizational level is known in ECM as the Agency level. Agencies are managed by an Administrator (or Chief). Examples include the Forest Service, the Food Safety Inspection Service, and the Rural Housing Service. Offices within the Assistant Secretariats are at this level. Examples include the Office of Civil Rights and the Office of Operations.

Division Level: The fourth organizational level is known in ECM as the Division level. This level, and its title, differs widely within USDA based on the organization of a particular agency. In some agencies, this organizational level is the Deputy Administrator level.

Groups and Positions

Users in ECM are assigned to Groups. Users may belong to many groups. One group is designated as the user's Default Group.

When a task is assigned to a ECM Group, it is, in effect, assigned to every member of that group and initially appears in the Inbox of each member of the group. The task status is set to Assigned. Once a member selects the task for action, it is removed from the inboxes of the remaining members of the group, and its status is set to Started. Should the user decide to return the task to the entire group, it can be Put Back.

A Position is a special type of Group that is related to a business role. Users can be assigned to Positions as they are assigned to Groups.

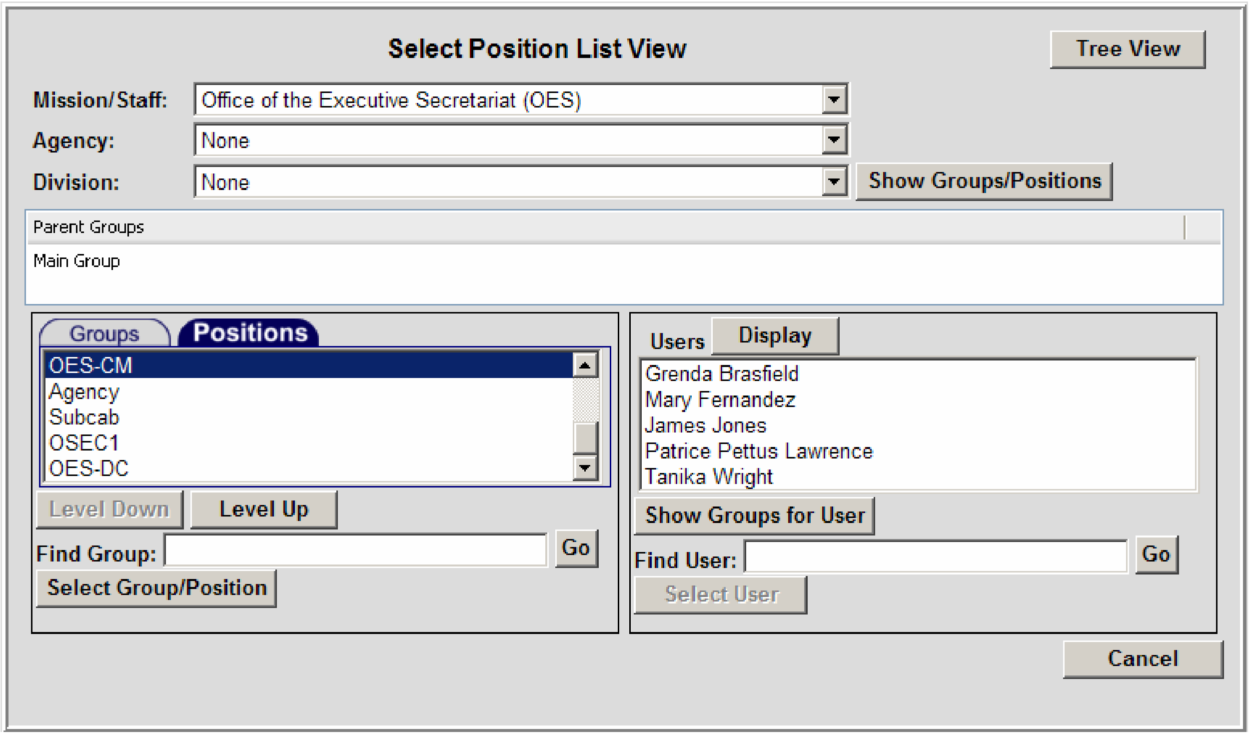


Figure 41: Select Position List View

What Are "Main" Groups?

A "Main Group" in ECM is a special, system-generated group that includes all users in each "division" of the ECM hierarchy. Every group in the organization must have a defined Mission/Staff, Agency, and Division. Each Division includes a main group that includes all users in that Division and all of its subordinate groups.

It is not recommended that "Main Groups" be designated as folder owners or as authorized groups.

What Are "None" Groups?

A "None" group is a special group, or place holder, that identifies a level of the organization with no valid entry. For example, a user assigned to the ***Mission Area*** Farm and Foreign Agricultural Services (FFAS), ***Agency*** Farm Service Agency (FSA), and ***Division*** Deputy Administrator for Commodity Operations (DACO) will be in the "Main Group" OSEC/FFAS/FSA/DACO/MG.

To identify a user who is assigned to the mission area itself—that is, a user assigned to the Office of the Under Secretary for Farm and Foreign Agricultural Services (FFAS)—there is no agency or division. For system reasons, a null or "none" group is created at those levels to keep the organizational structure parallel. Therefore, the user would be assigned to ***Mission Area*** Farm and Foreign Agricultural Services (FFAS), ***Agency*** None (N), and ***Division*** None (N), Main Group, or OSEC/FFAS/N/N/MG.

Navigating the USDA Hierarchy in ECM

In the ECM application, users have two options for navigating the organizational hierarchy to locate and select groups, positions, and users:

- **List View,** in which the user navigates through the hierarchy of organizations and groups displayed as lists, and
- **Tree View,** which allows the user to navigate using a tree-view. The tree view functions in a way similar to that used by the Windows Explorer interface.

These options are provided for all screens that need to select groups, positions, and/or users. The Personal Profile Screen allows the user to select either view as a user's default preference. The user also has the option to switch from List View to Tree View and vice versa by clicking the **TREE VIEW** or **LIST VIEW** button on the right of the screen.

List and Tree Views

Two views of the organizational hierarchy are available, the "List View" and the "Tree View."

List View

The "List View" screen is the basic screen used to select a group, position, or user. There are two versions of the list view.

The basic version, displayed in the figure below, includes drop-down lists for Mission/Staff, Agency, and Division, and navigation buttons for locating and selecting subordinate groups, positions, and users.

In the example below, Farm and Foreign Agricultural Services (FFAS) has been selected as the Mission/Staff level, the Farm Service Agency has been selected as the Agency, and the Deputy Administrator for Commodity Operations has been selected as the Division.

Select the Mission/Staff level first. Once the Mission/Staff level has been selected, only appropriate choices are available in the Agency level list. Once the Agency has been identified, the appropriate Divisions are displayed in the Division list.

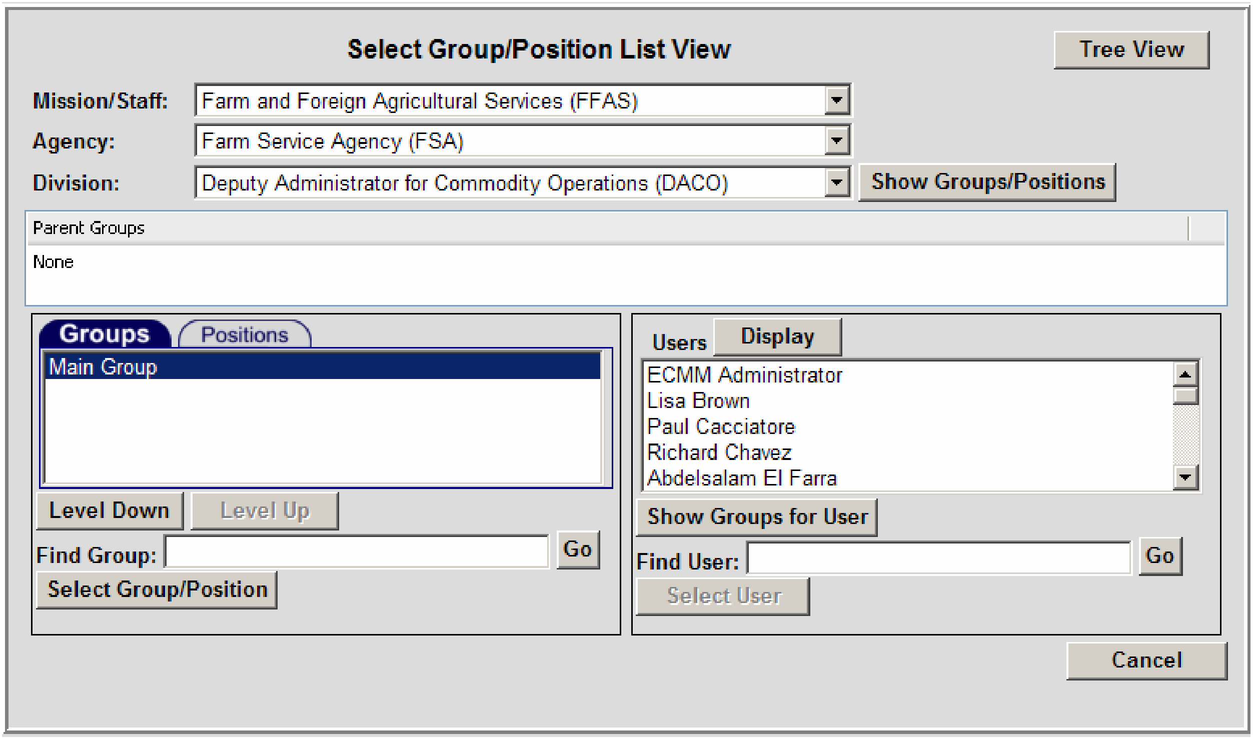


Figure 42: Select Group/Position List View

Once the three upper levels have been defined, click on the **SHOW GROUPS/POSITIONS** button. This will display the Division's "Main Group." To display the users in the "Main Group," click on the **DISPLAY** button in the User pane.

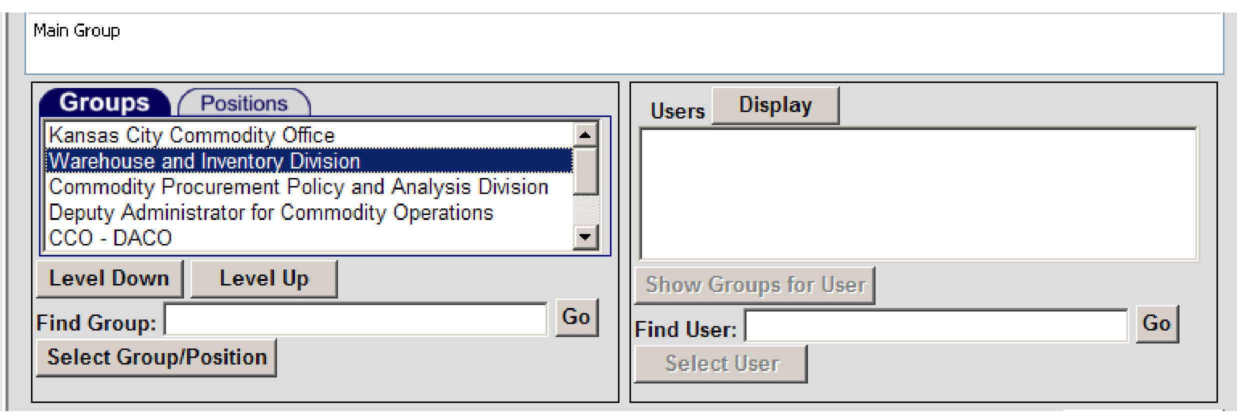


Figure 43: Select Group/Position List View (Level Down)

To navigate to subordinate groups in the division, click on the **Level Down** button. The subordinate groups are displayed. To navigate further, use the **Level Down** or **Level Up** buttons. To select a subordinate group—in this example, the Warehouse and Inventory Division—use the **Select Group/Position** button.

Enhanced List View

When the list view is called in certain functions—for example, when defining an organizational level for a privileged user—a modified version of the List View is used. Note that only the top three organizational levels are displayed unless the **More** button is clicked.

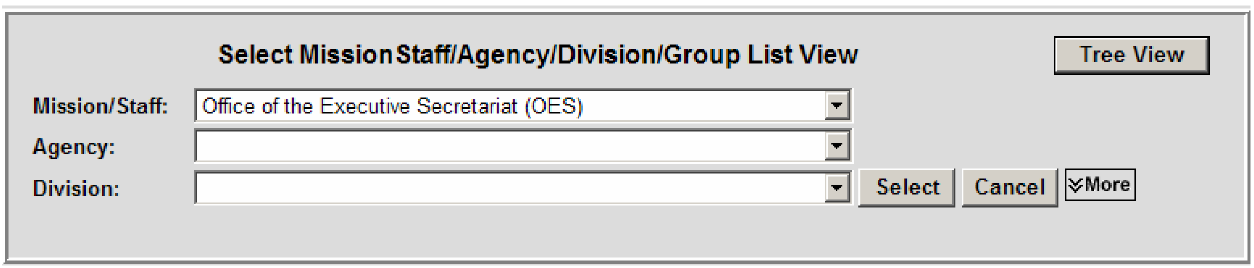


Figure 44: Select Mission Staff/Agency/Division/Group List View (Less)

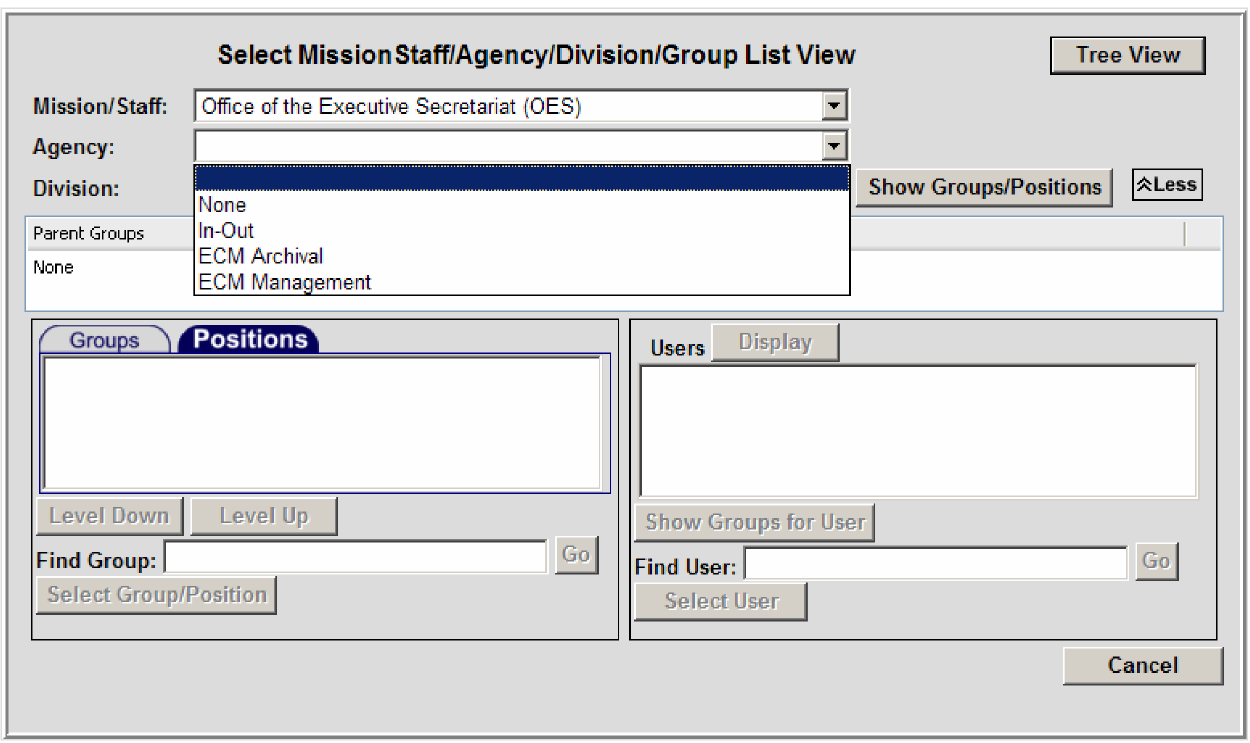


Figure 45: Select Mission Staff/Agency/Division/Group List View (More: Select Division)

In either the Less or More views, use the drop-down lists to select the appropriate Mission/Staff, Agency, and Division.

Most ECM functions and attributes must be attached to a user or to a group within a division. A group attached to a Mission/Staff level is assigned to an Agency of "None" and a Division of "None."

Some functions and privileges can now be attached directly to a Mission/Staff, Agency, or Division. These functions call the enhanced list view.

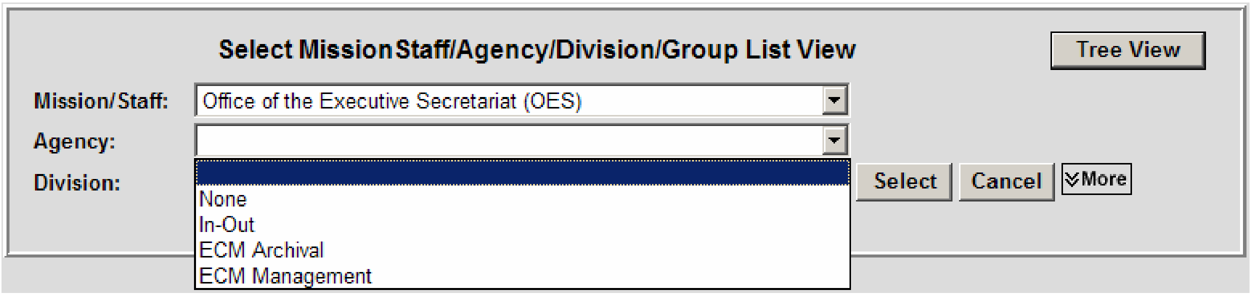


Figure 46: Select Mission Staff/Agency/Division/Group List View (Select Division)

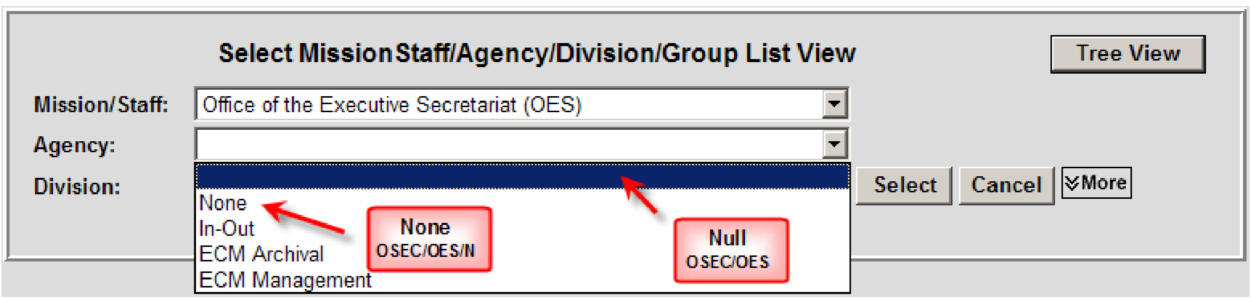


Figure 47: Select Mission Staff/Agency/Division/Group List View (Select Division None vs. Null)

In the example above, note that the "Agency" can be defined as the system group "None" or one of the three named Agency-level groups. However, the Agency level can also be left blank (null). If left null, the privilege is attached to the Office of the Executive Secretariat group itself.

Tree View:

The same tasks that can be completed using the List View can be accomplished using the Tree View. From the List View screen, click the **TREE VIEW** button. To return to the List View from the Tree View, click the **LIST VIEW** button.

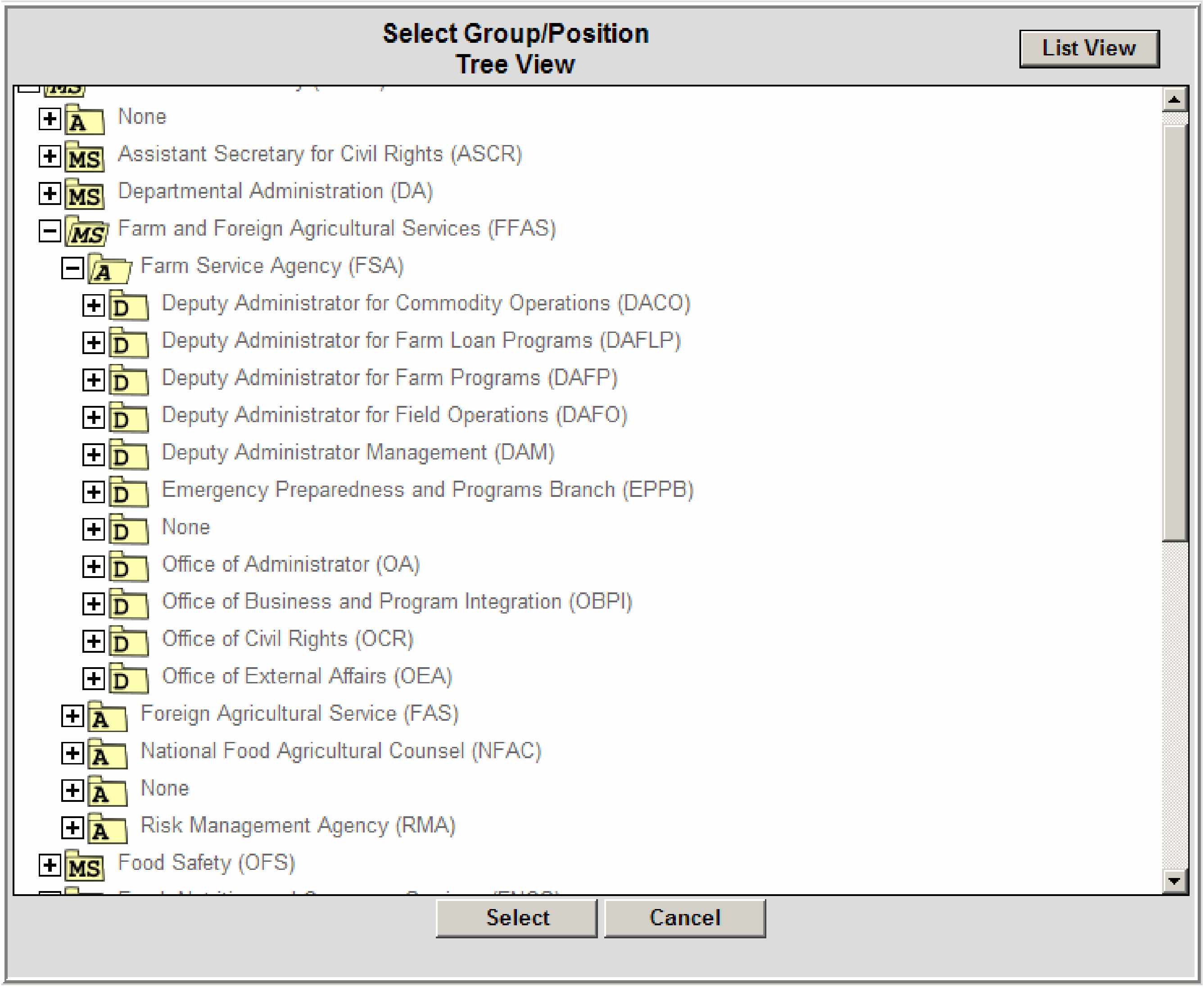


Figure 48: Select Group/Position List View

To access the Tree View interface, the user clicks the <Tree View> button. The Tree View is shown above. Each group is defined at an organizational level. Folder icons have letters to indicate their level. Folder icons include:

MS – Mission/Staff (for example Farm and Foreign Agricultural Services (FFAS))
A – Agency (for example Farm Service Agency (FSA))
D – Division (for example, Deputy Administrator for Commodity Operations (DACO))
G – Group
P – Position

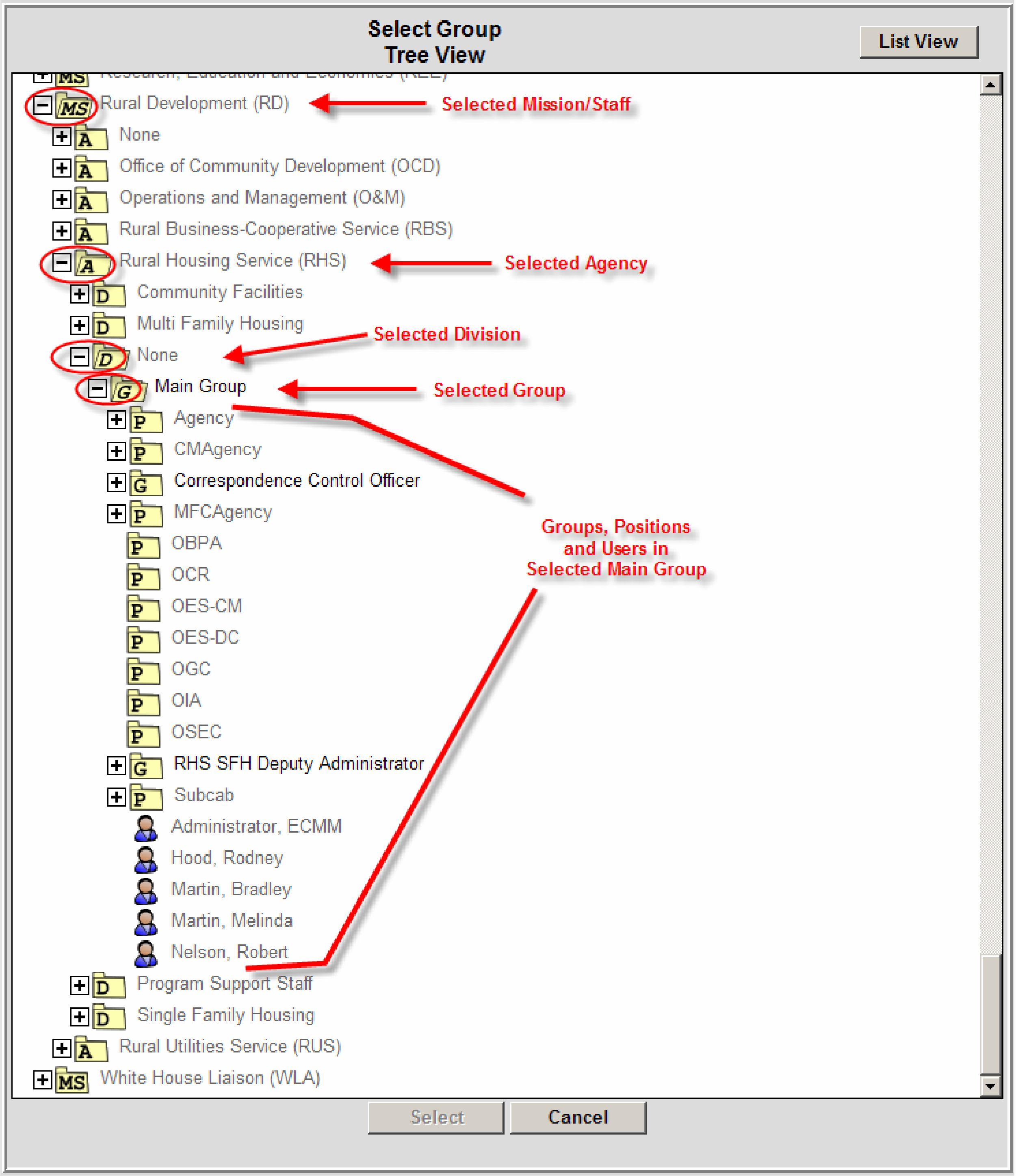


Figure 49: Select Group/Position Tree View

The organization hierarchy is shown as folders and person icons. Person icons are names of individual users. To see more detail within a level, the user clicks the <+> operator. To see less detail, the user clicks the <-> operator. To make a selection, the user highlights the desired Group, Position, or User and clicks the <Select> button.

Adding and Modifying Groups

To add or modify an ECM group, select the “Groups/Positions” link on the Administration Menu.

Figure 50: Administration Menu (Groups/Positions)

The procedures for adding or modifying a group or position are similar.

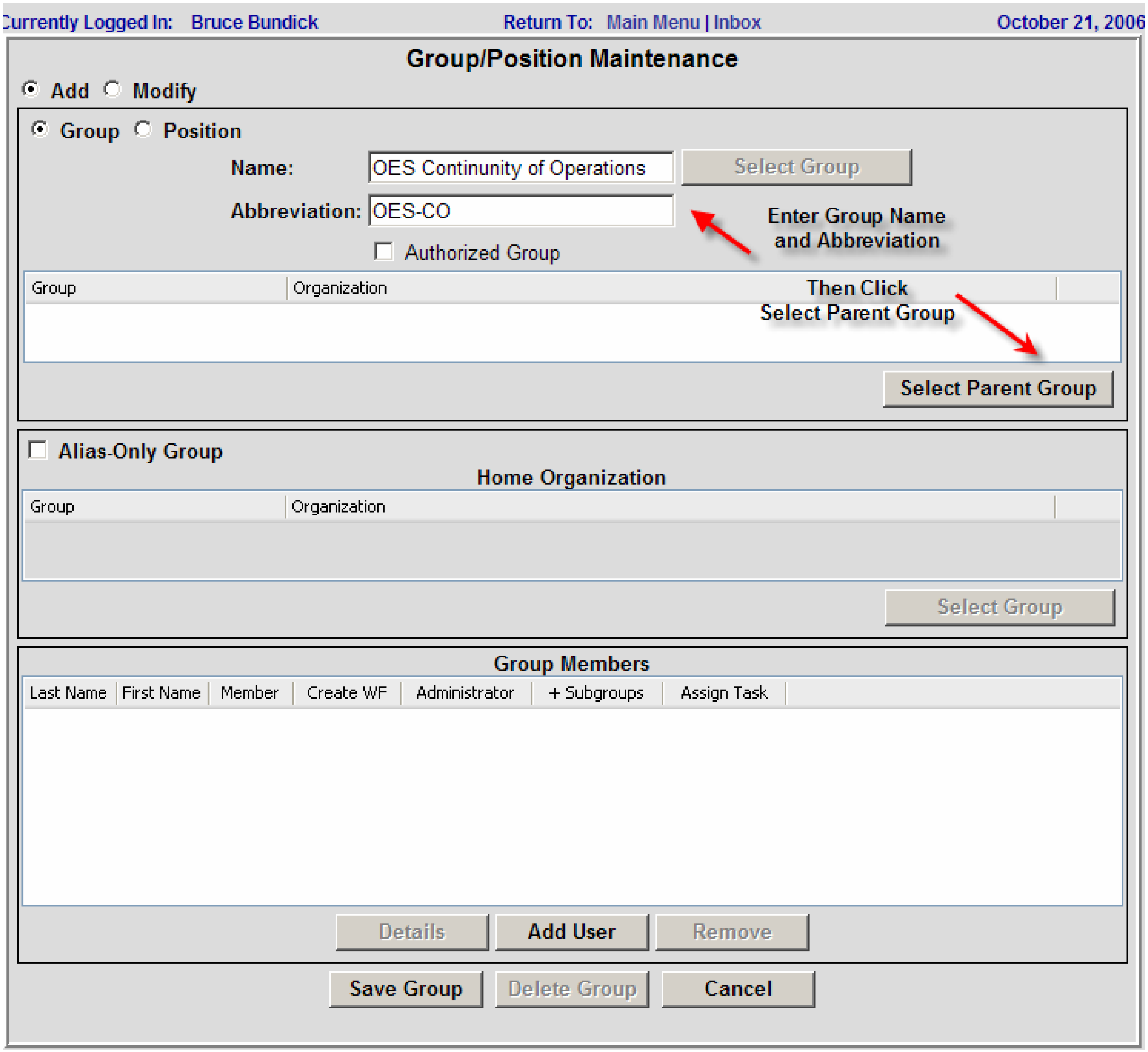


Figure 51: Group/Position Maintenance

On the Group/Position Maintenance screen, use the radio buttons to select Add or Modify and Group or Position. To add a group or position, enter the name and abbreviation, and then click "Select Parent Group."

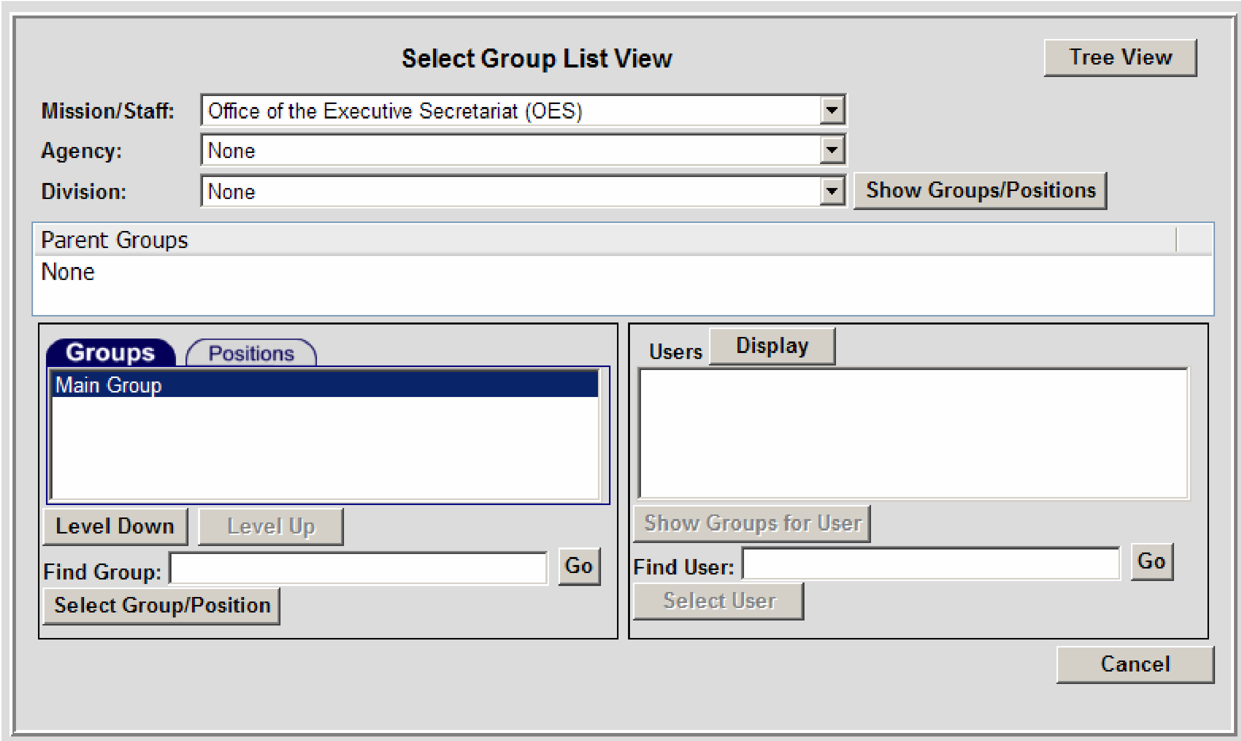


Figure 52: Select Group List View

Select the appropriate parent group for a group to be added, or if modifying a group, select that group. The Select Group/Position button returns the user to the Group/Position Maintenance screen.

The lower panel on the Group/Position Maintenance screen can be used to perform other group or position administrative tasks, for example, adding users, removing users, or assigning group privileges.

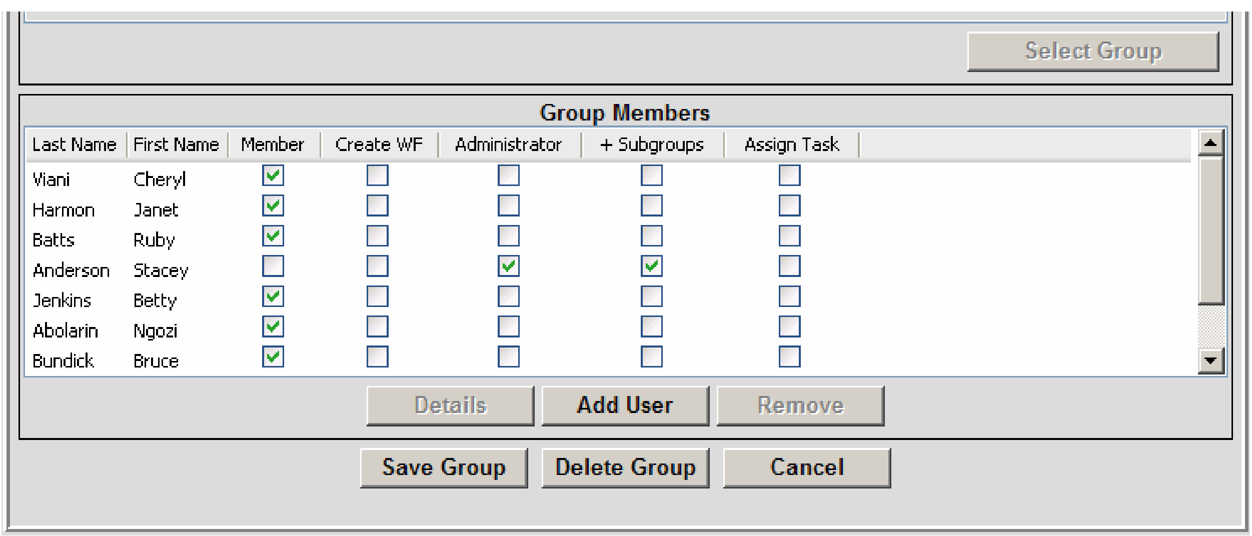


Figure 53: Group/Position Maintenance (Manage Group Users)

Adding and Modifying Users

From the Main Menu select the Administration link.

Figure 54: Main Menu Administration Link

On the Administration Menu, select the Users link.

Figure 55: Administration Menu Users Link

Selecting this option opens the User Maintenance Screen. This screen provides authorized administrators with the ability to add users, make the active or inactive, assign users to groups, etc. Only Security Officers can designate Application Administrators, Module Administrators, Agency Group Administrators, or Privileged Users.

Adding A New User to ECM

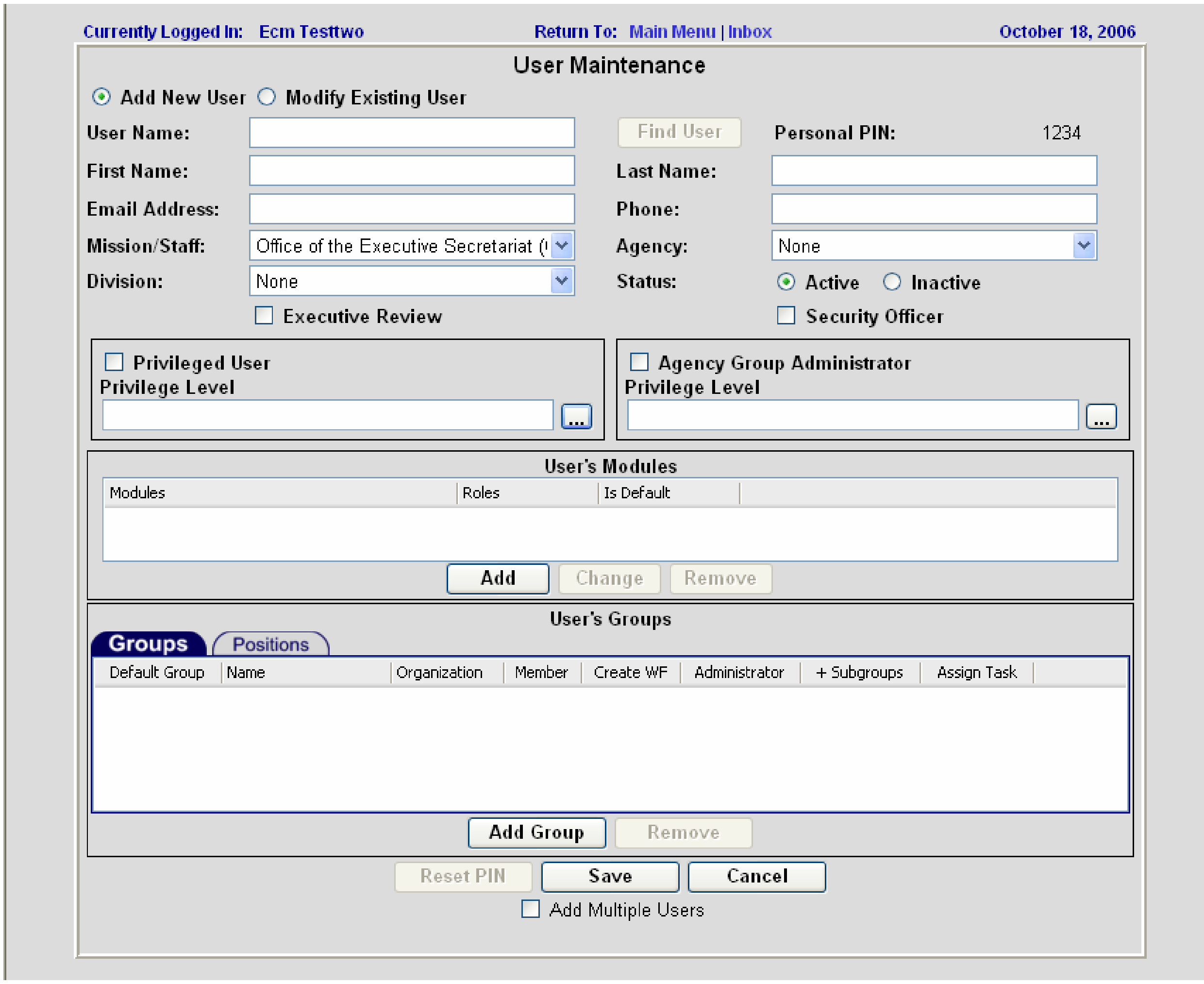
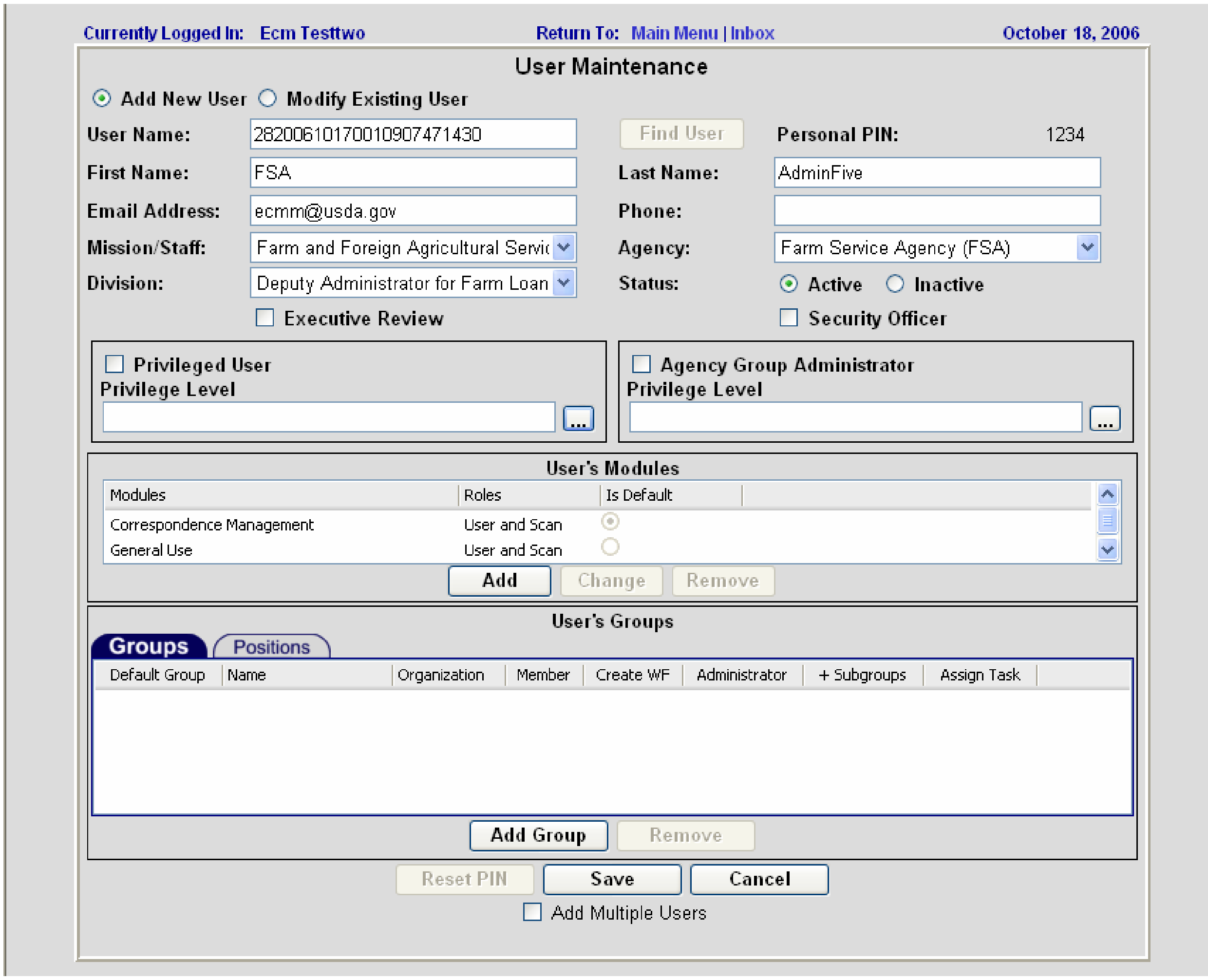


Figure 56: User Maintenance (Add New User)

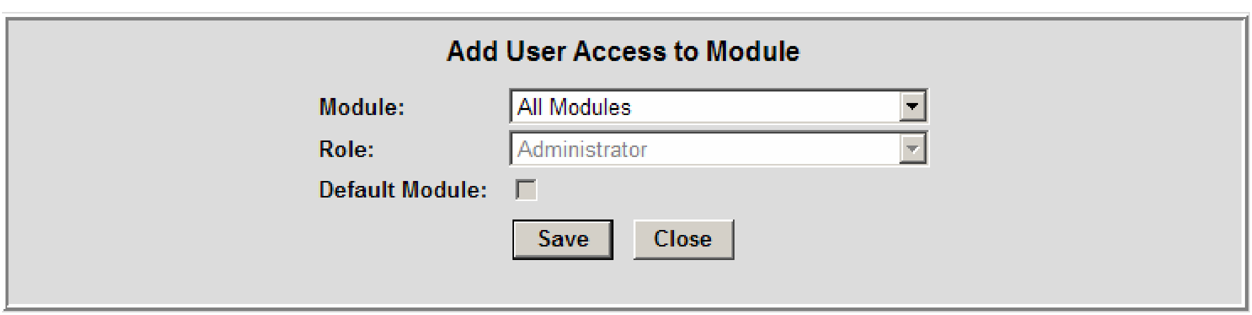
Before a user can be added to ECM, the user must have an active, Level II eAuthentication account. The administrator must have access to the user's eAuthentication identification number. Currently, this is captured in an error message generated when a user with eAuthentication credentials but yet not enrolled in ECM attempts to log in to the application. This information can also be obtained through an eAuthentication LRA (local registration authority agent).

On the User Maintenance Screen, populate the following fields:

* User Name (the e-authentication unique identifying number)
* First name
* Last name
* E-mail address



Select the default Mission Staff, Agency, and Division of the user from the drop-down lists. After that is selected, click on the Add button under User's Modules. This will open up the Add User Access to Module Screen. From the drop-down list, select the appropriate User Module and Role. Select the Default Module box if applicable. Save.



After the Module has been added, the administrator will return to the User Maintenance Screen.

Users must belong to at least one group. Users are automatically added to the Main Group of their default Mission/Staff/Agency/Division. If the user needs to be added to one (or more) additional groups, click the **ADD GROUP** button.

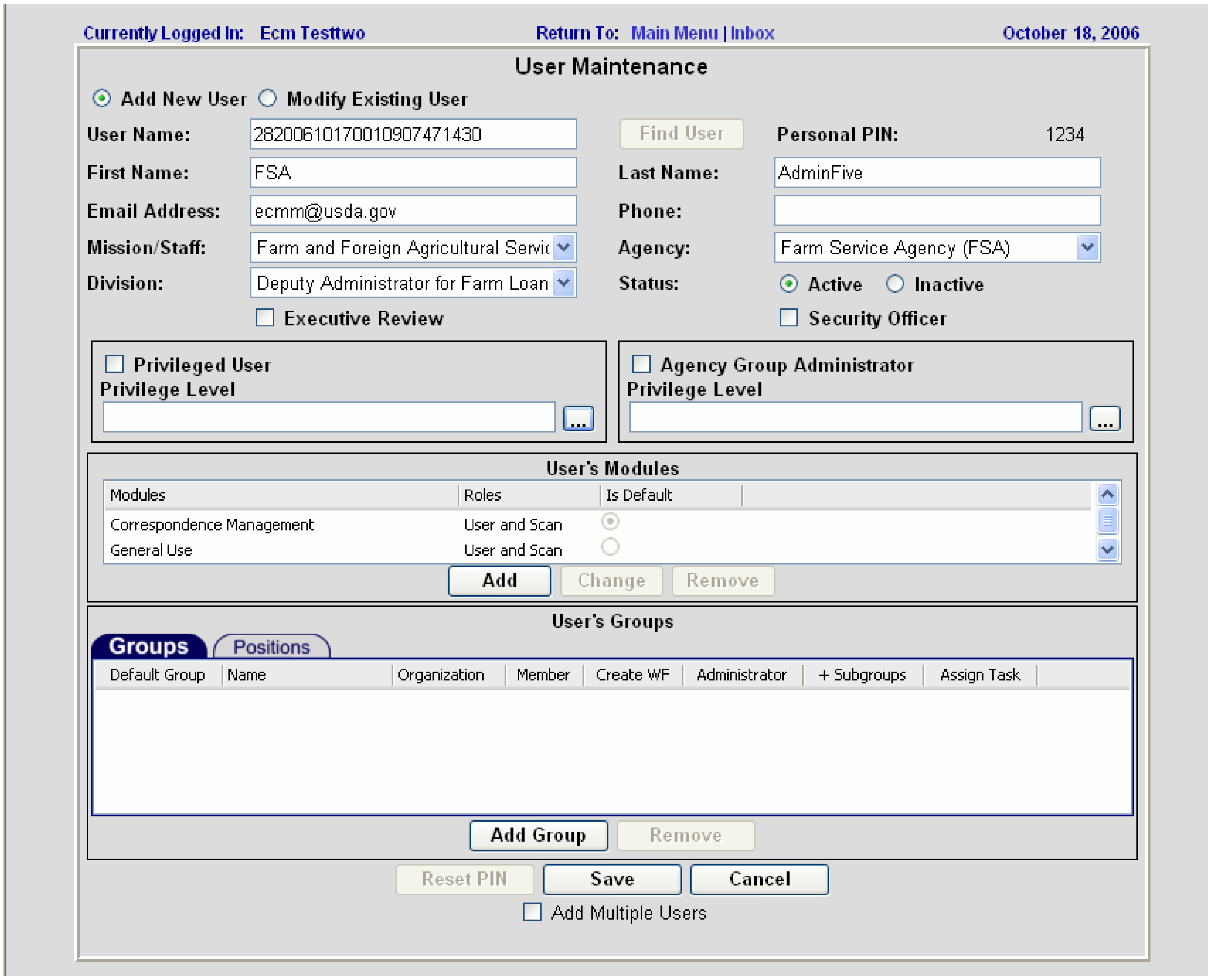


Figure 57: User Maintenance (Add New User)

This will open the Select Group/Position screen. Either the List View (shown below) or the Tree View can be used to select the additional group(s).

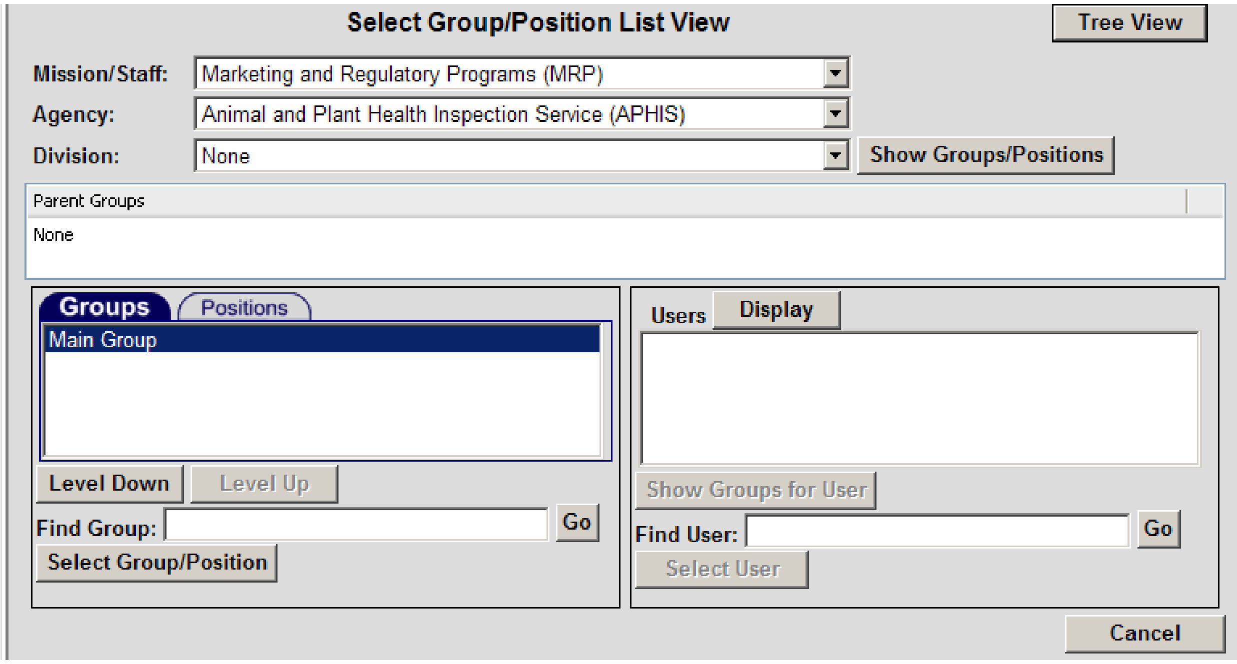


Figure 58: Select Group/Position List View

Once the group(s) has been added, you will need to assign the user the appropriate rights within the group. This is accomplished by checking the appropriate boxes. Members receive tasks assigned to the group. Create WF allows the user to save workflows to the group workflow library, a privilege otherwise restricted to administrators. The Administrator box designates the user as a Group Administrator for the group. If the +Subgroups box is checked, the user also has administrative rights for subgroups (child groups). The Assign Tasks privilege allows the user to designate a member of a group as the assignee of a task. (Despite the designation, the task appears in the inbox of every Member of the assigned Group.)

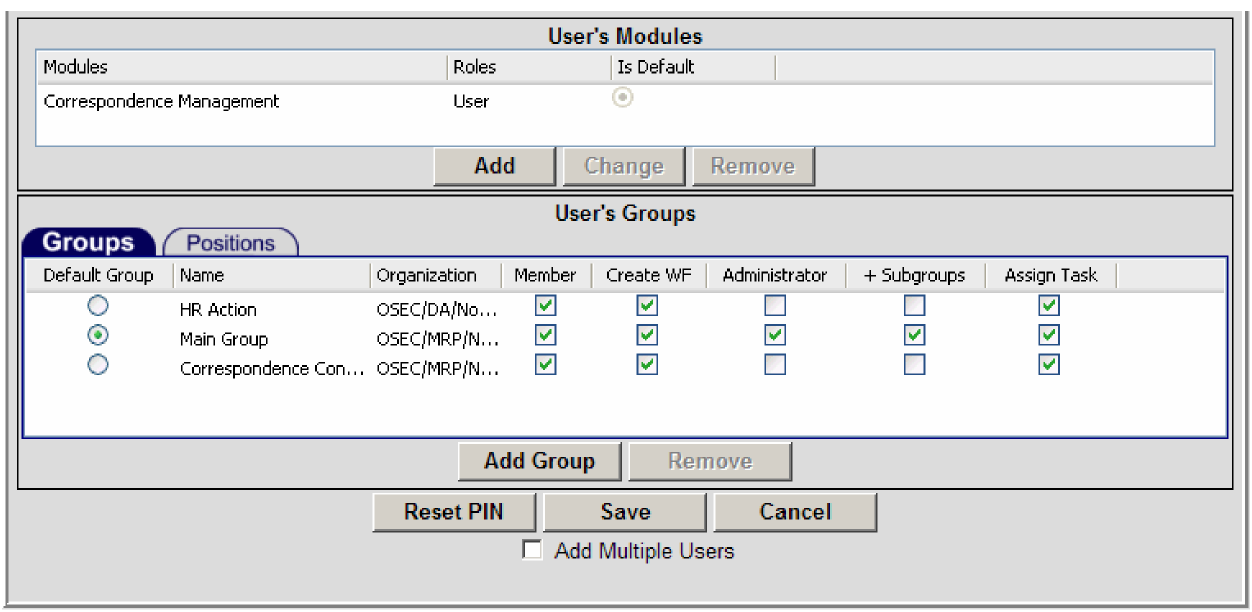


Figure 59: User Maintenance (Add or Change User's Groups)

4. Creating a Customized List of Values

ECM Lists of Values

There are many lists in the ECM application. Most such lists can only be changed by Application or Module Administrators.

Application Administrators only can add or change the list of U.S. Holidays or add or change the Mission/Staff, Agency, or Division levels of the organizational hierarchy. Application Administrators and Module Administrators can add or change Address Book Location Descriptions, Folder Set Up Groups, Categories, VIP Types, and Special Instructions.

There are three special lists, called lists of values, that can be anchored at any point in the organizational hierarchy and apply to all organizations and groups below that point in the hierarchy (unless overridden at a lower level). They are Subjects, Document Types, and Task Descriptions. Accordingly, users may see different lists of values depending upon their location in the hierarchy.

Each module has a default list established. By default, every group within ECM uses the default module group unless that group, or a parent group, owns a different list. Such local lists can be created or changed by all classes of administrator, although Agency Group Administrators and Group Administrators can create or change a list only if they have administrative privileges for the target group OR for a parent of that group.

For example, assume no organization had created its own specialized list of Document Types, FFAS had created a specialized Mission Area subject list, and FSA created specialized list of Task Descriptions.

A user creating a folder in FSA would see the generic module (USDA) list of Document Types, the FFAS list of subjects, and its own specialized list of Task Descriptions. A user creating a folder in FFAS would see the generic module lists of Document Types and Task Descriptions and the FFAS list of subjects.

A list of values may be attached to any group and managed by any administrator with administrative rights for that group.

Creating or Changing a List of Values

General Information

All entries in any list of the three lists of values must reside in the ECM master list for that value. Accordingly, to add an item to a list of values, it must be first added to the ECM master list.

A local list may adopt a default list and supplement it with its own entries, or it may include only items not included on any parent list, or it may be a combination of inherited and new items.

Editing a List of Values

Navigate to the Main Menu and select the link to the Administration Menu.

Figure 60: Administration Link on ECM Main Menu

Select one of the List of Values items (Subjects, Document Types, Task Descriptions) for editing.

Figure 61

As an example, we will create a new list of Task Descriptions for Rural Developments' Chief Information Officer. Selecting the "Task Descriptions" link on the Administration Menu will open the Module/Group List Maintenance Screen displayed below.

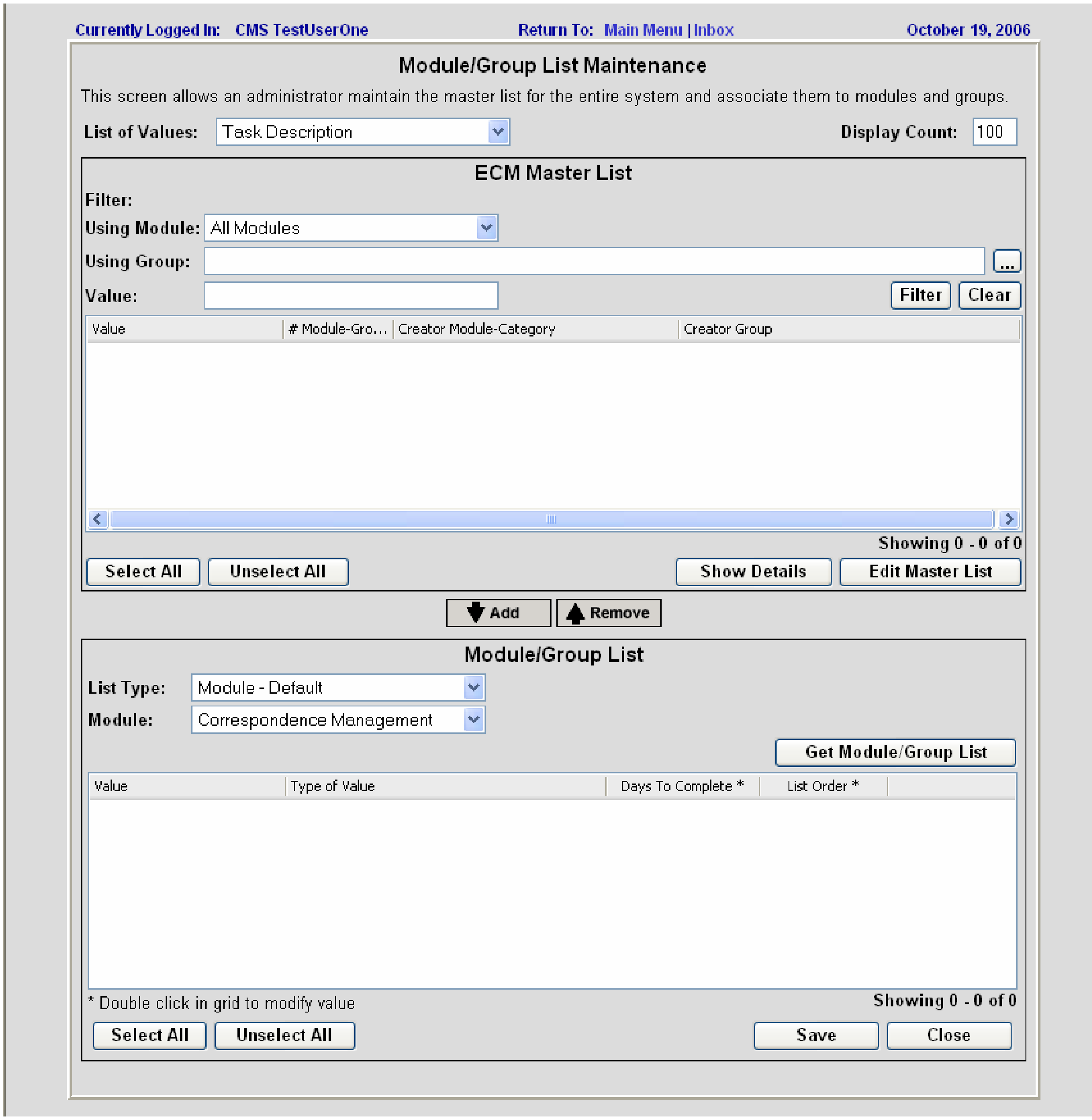


Figure 62: List of Values: Module/Group List Maintenance Screen

Note that the screen lists "Task Description" as the List of Values to be edited. The upper panel of the screen displays the ECM Master List items. The master list includes all items currently in use on any list in the application (as well as some former items no longer in use).

The bottom panel displays the module or group list to be edited.

To begin, click on the **FILTER** button to display all Task Descriptions currently available on the master list. The "filters" (Using Module; Using Group; and, Value) permit display of a portion of a long or complicated list, for example, subjects.

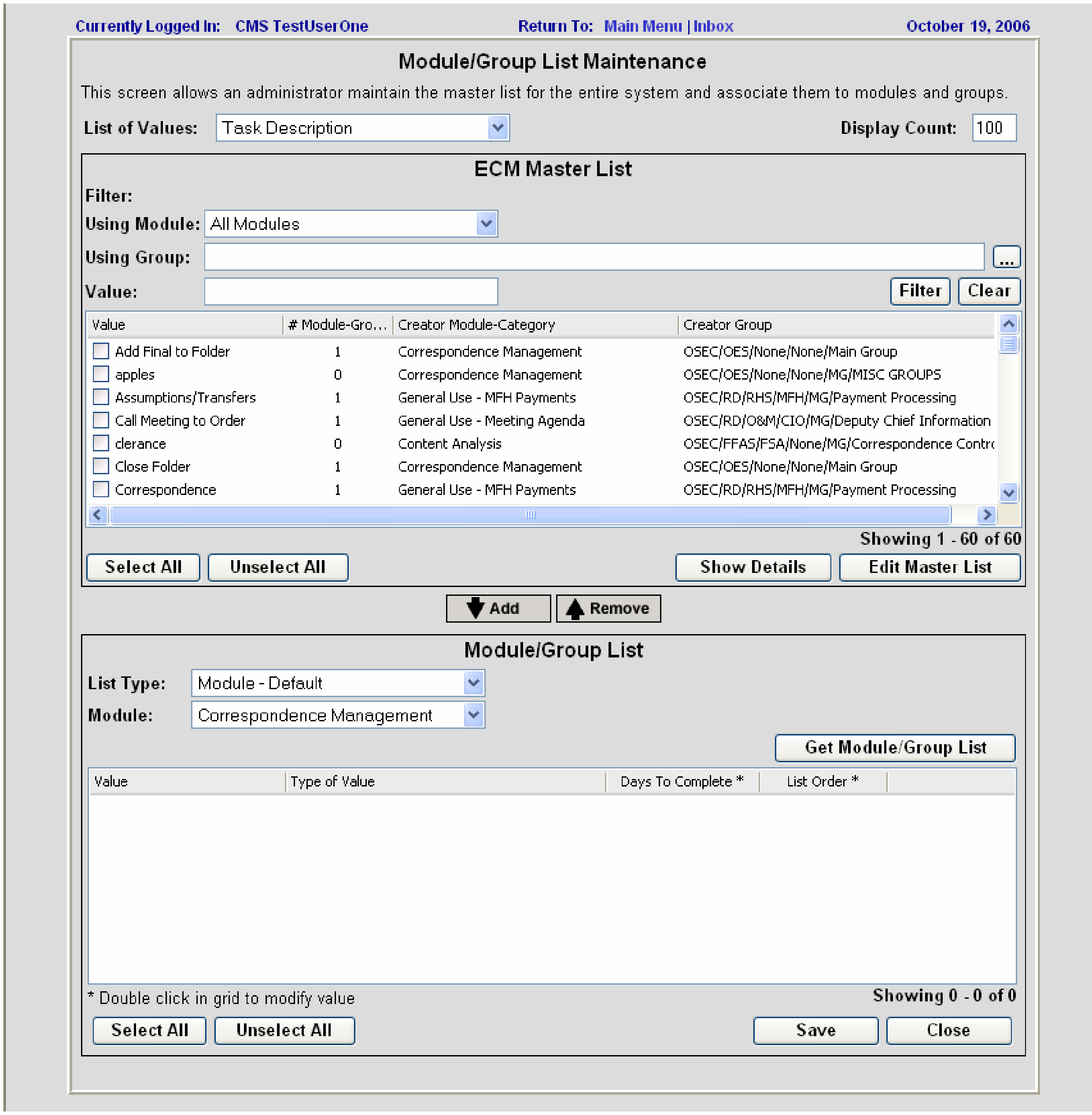


Figure 63: List of Values: Retrieving the ECM Master List

In order to make a customized list for your group, scroll down and click Group Customized from the List Type drop-down menu. Select the Module for the customized List of Values. (If you select the General Use module, you will also need to select a Category.) Select the appropriate radio button, "Use Only Customized Values" (create a new list from scratch) or "Add

Customized Values to the Module-Default List of Values" (create a list by making a copy of the default list and adding your new values to that list).

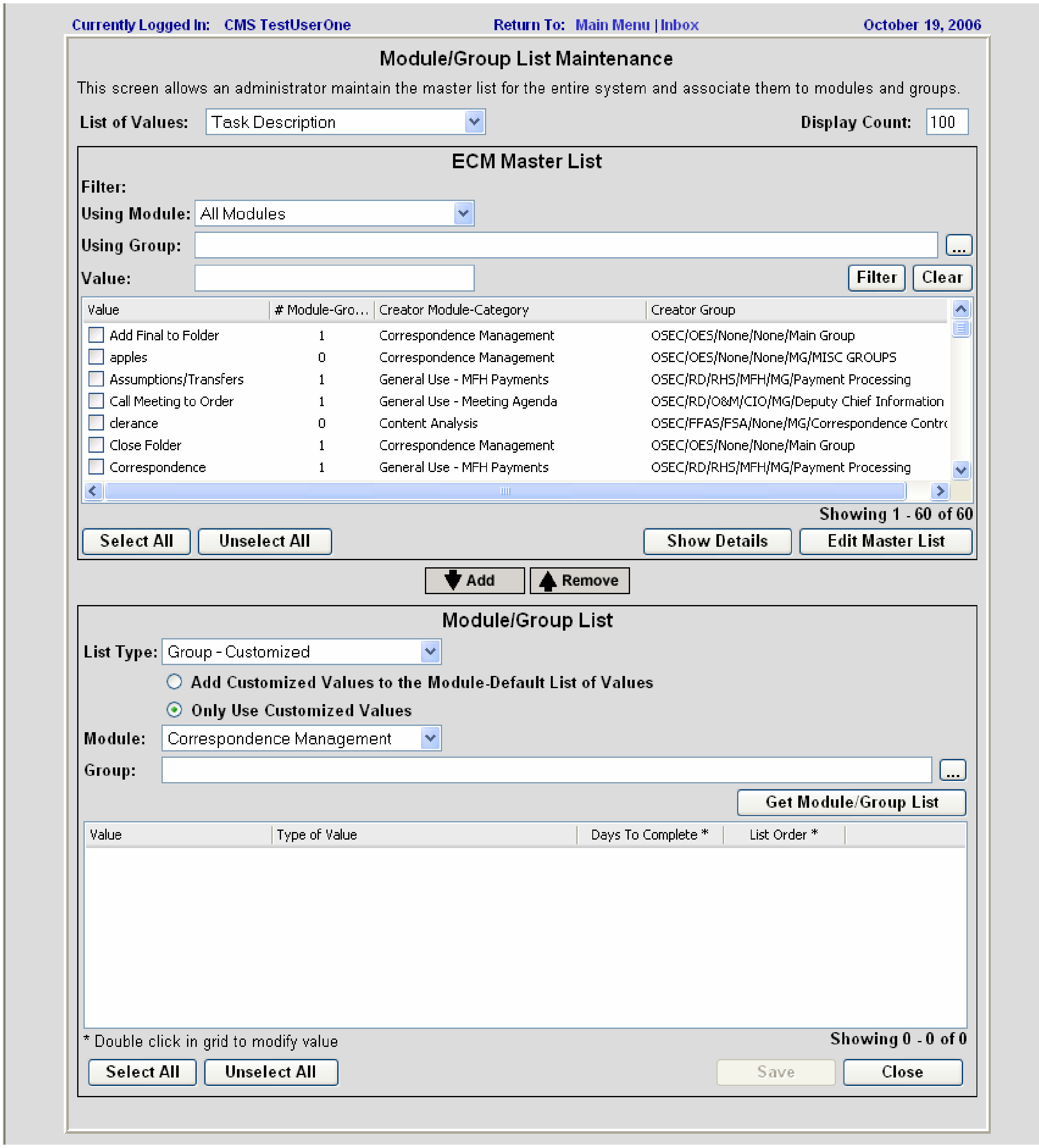


Figure 64: List of Values: Creating a Group-Customized List

Once this information is populated, click on the ellipsis button next to Group on the screen. This will open the "Select Mission/Agency/Division/Authorized Group" screen and start the process of identifying the group to which the new Task Description list of values will be attached. From this screen (the Tree View in the example below), highlight the appropriate group and click the **SELECT** button.

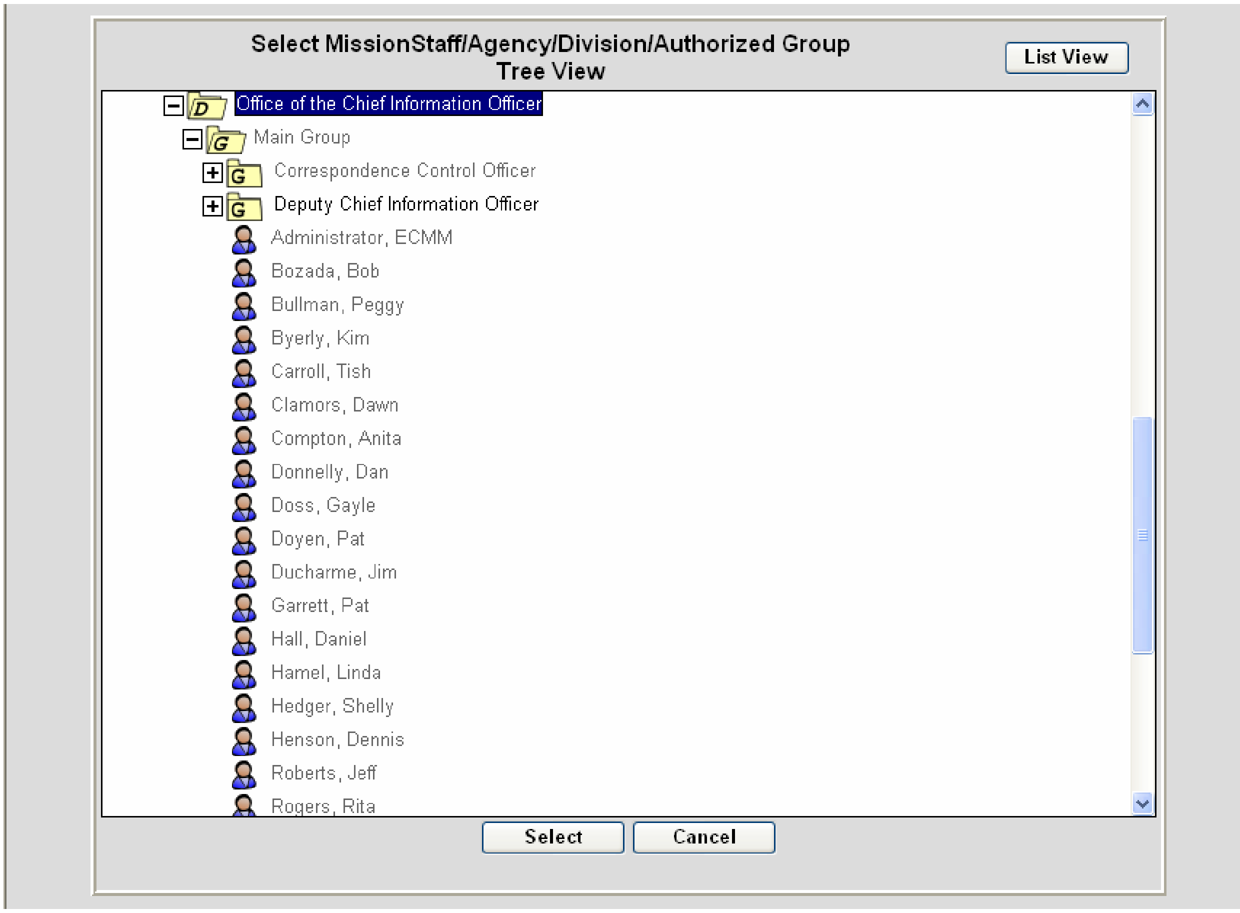


Figure 65: List of Values (Select Mission/Staff, Agency, and Division for List—Tree View)

Or in the List View:

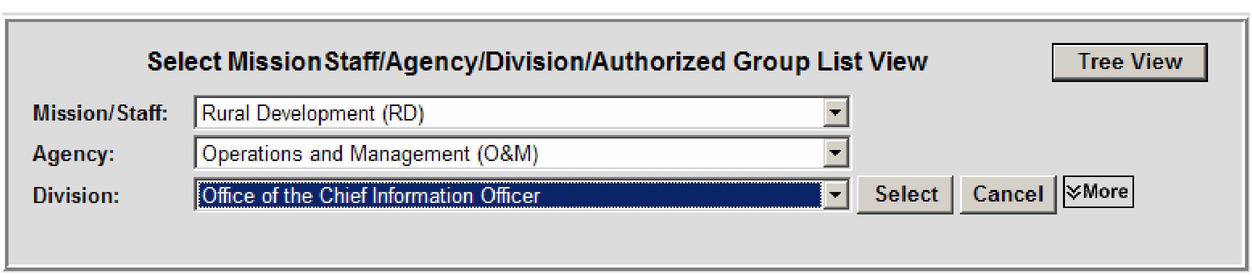


Figure 66: List of Values (Select Mission/Staff, Agency, and Division for List—List View)

Once the Group has been selected, and the Group is displayed in the Module/Group List pane, click on the **GET MODULE/GROUP LIST** button. If no items are displayed, this will verify that a customized List of Values does not already exist for the selected group.

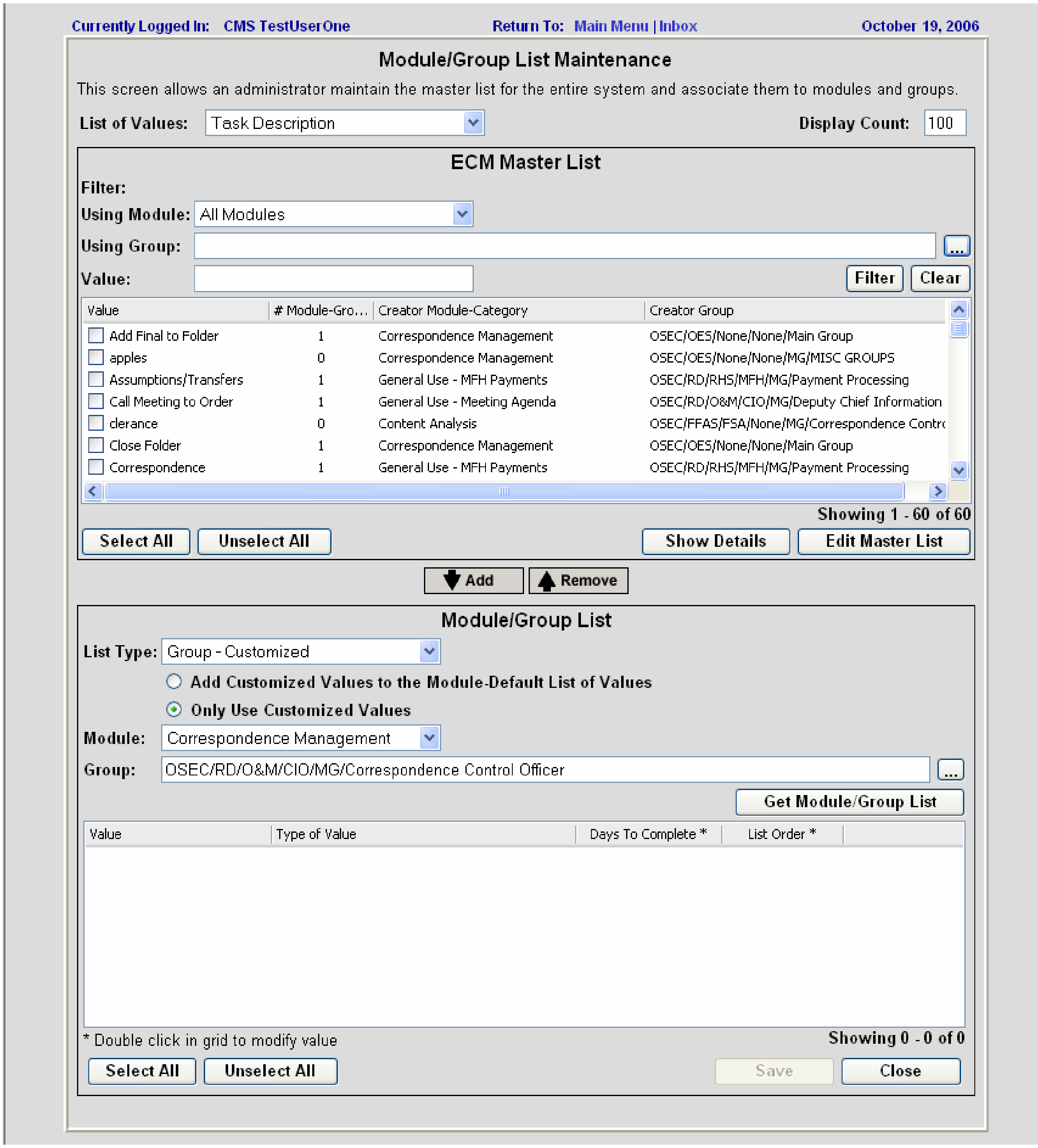


Figure 67: List of Values (Verifying Absence of Current Custom List of Values)

To create a customized list of values, add specific tasks from the ECM master list to the customized list. Select values from the master list by checking the box next to the Value and click the **ADD** button in the center of the screen. Items on the master list that you have checked will be added to the new customized list of values.

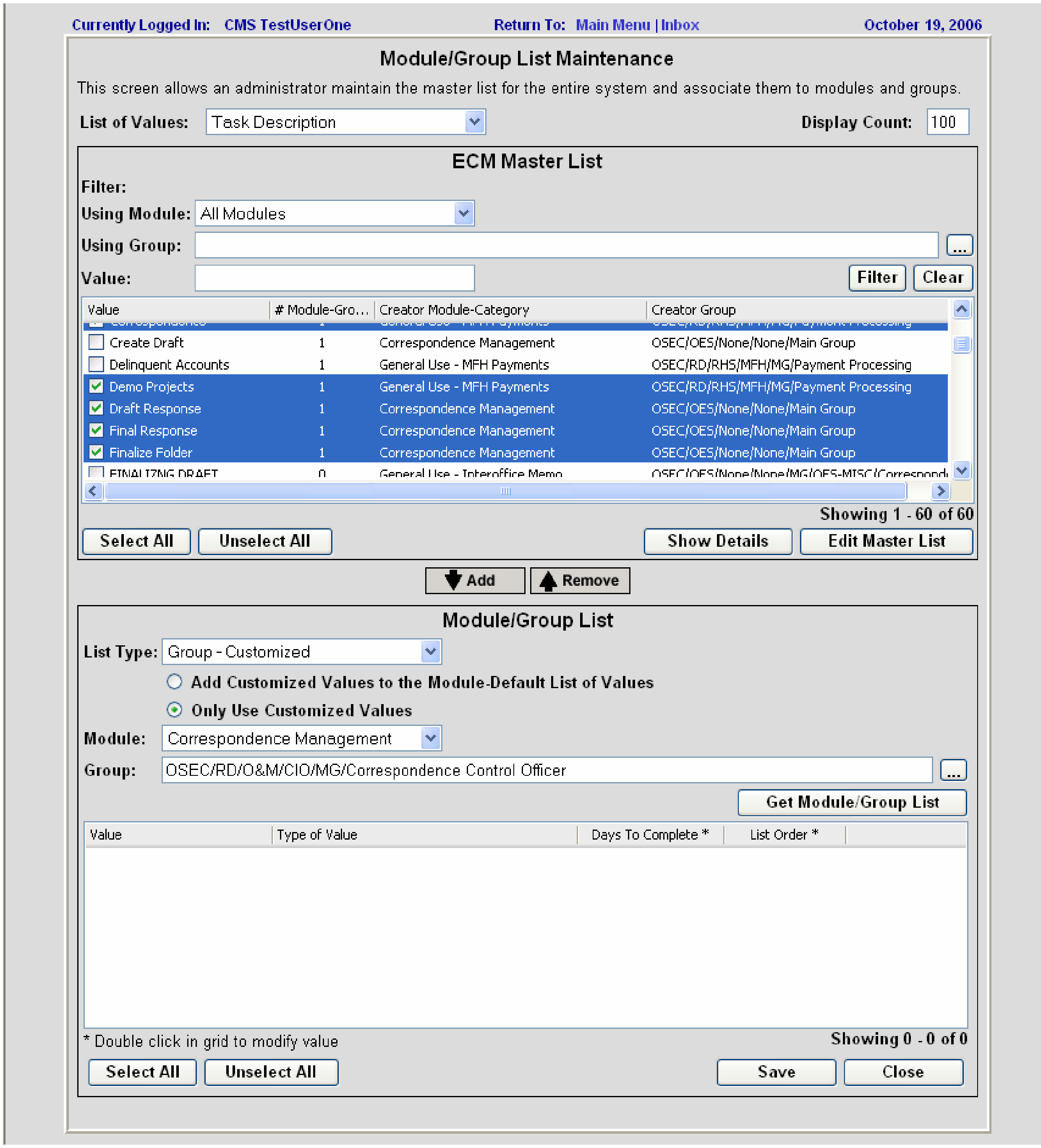


Figure 68: List of Values (Select Values from ECM Master List)

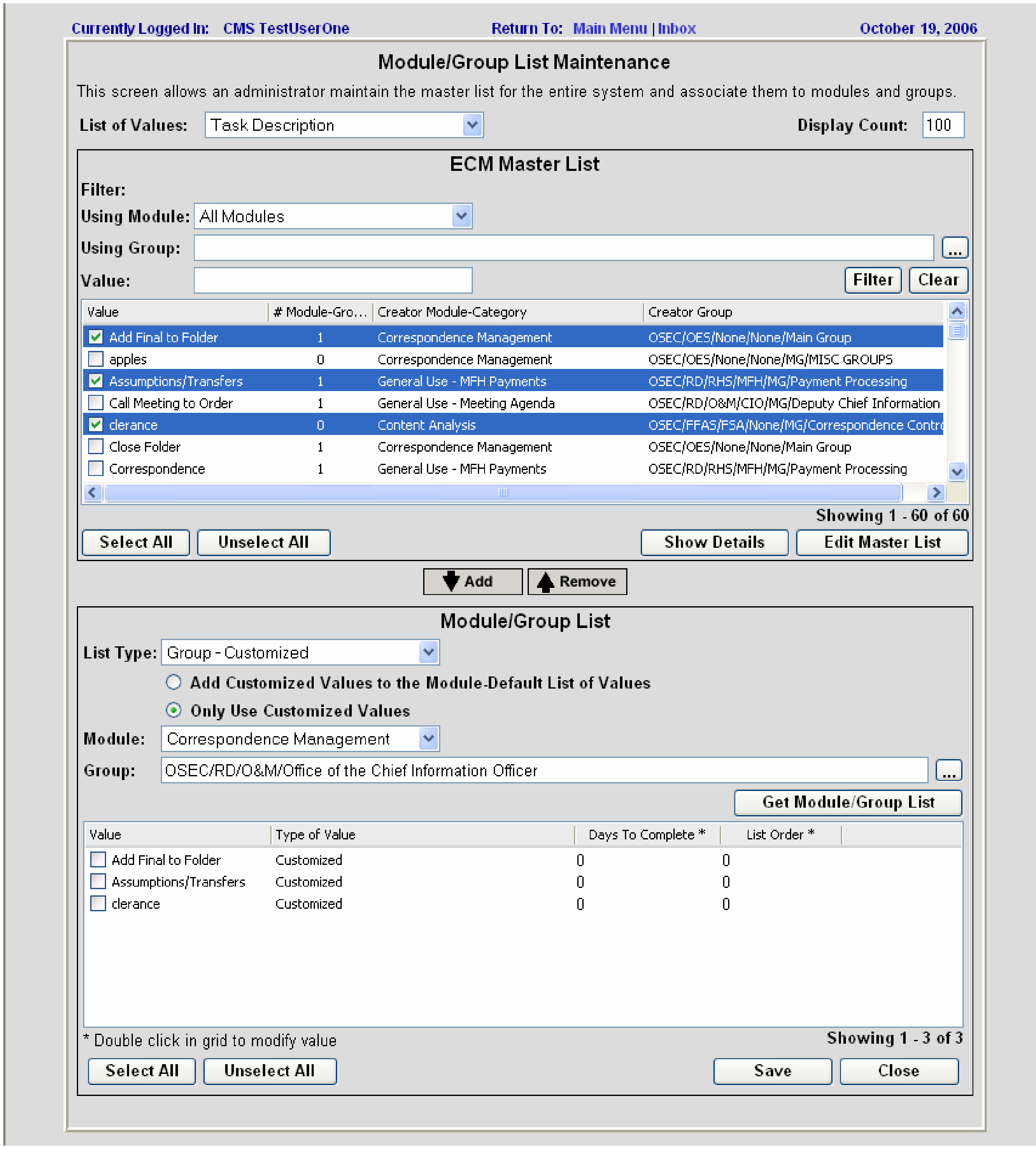


Figure 69: List of Values (Selected Items Added to New Customized List of Values)

To complete the customized list in this example, you need to enter a List Order and Days to Complete for each new task description on the customized list. The "List Order" values will determine the order in which the new task descriptions appear in the drop-down list when users use that list to add a value to a folder. The "Days To Complete" value defines the expected work period for the task that ECM will use in calculating due dates for the task. To edit the "Days To

Complete" and "List Order," click in the grid and type in the appropriate values. These values must be populated in order to save the new customized List of Values. Once new values have been entered, this is done, and click Save.

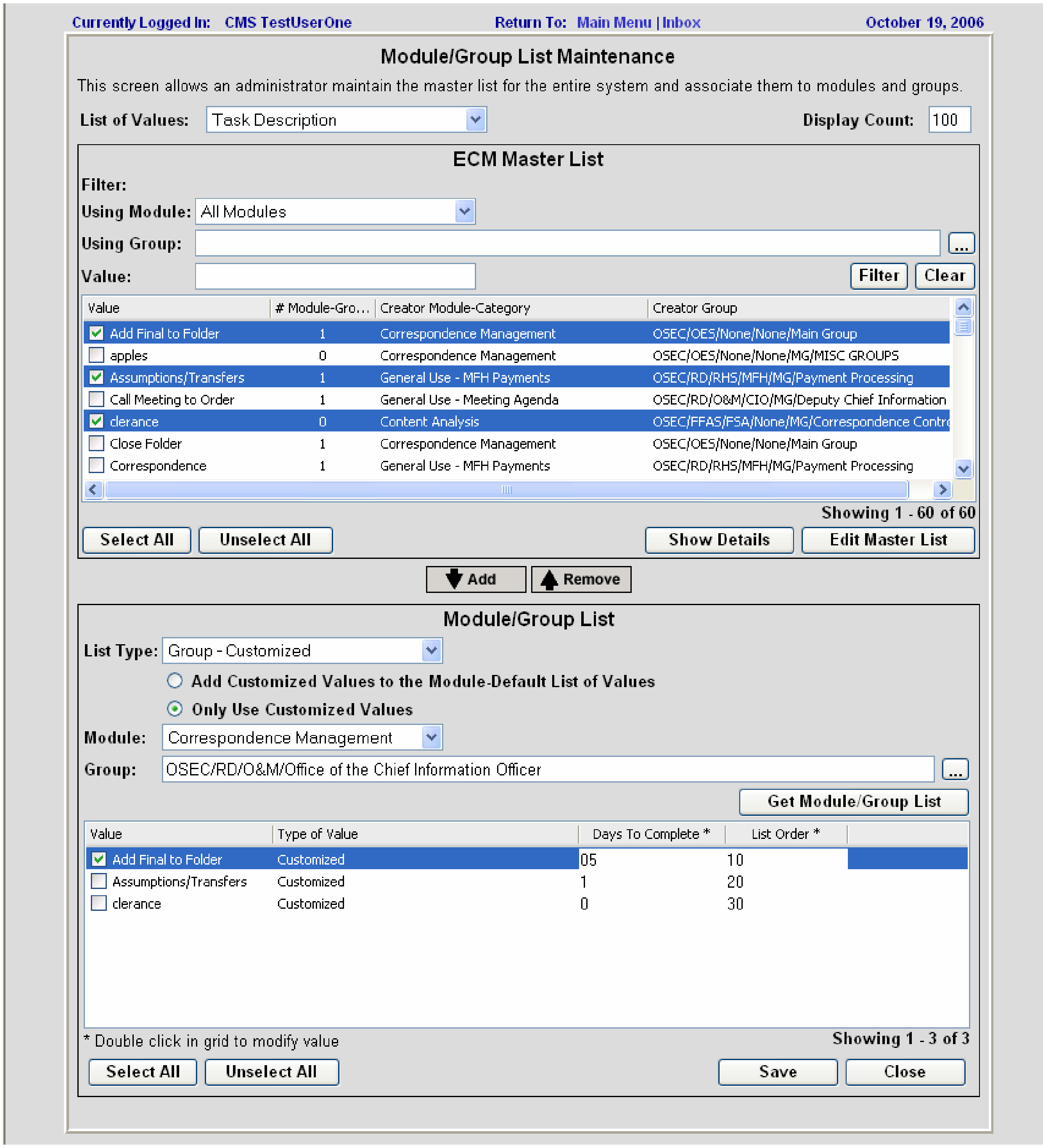


Figure 70: List of Values (Days to Complete/List Order Added to New Customized List of Values):

If your business process requires a value for Task Description that does not currently exist in ECM, you will need to add that value to the ECM Master List in order to make it available for your customized list.

To add a value to the Master List, Click on Edit Master List on the Module Group List Screen. This will open up the Add/Update Master List screen.

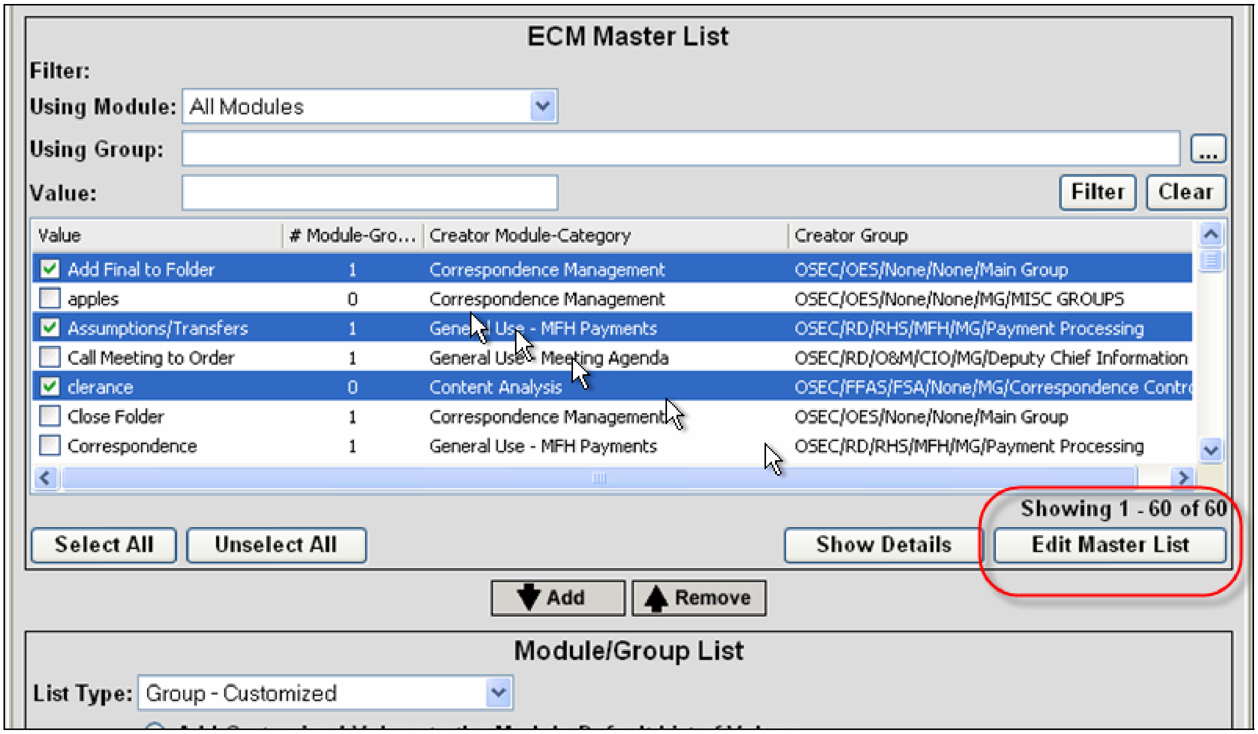


Figure 71: List of Values (Edit Master List)

This opens the Add/Update Master List screen. This screen allows an authorized user to add items to the ECM Master List, which in turn makes them available for use on a customized list.

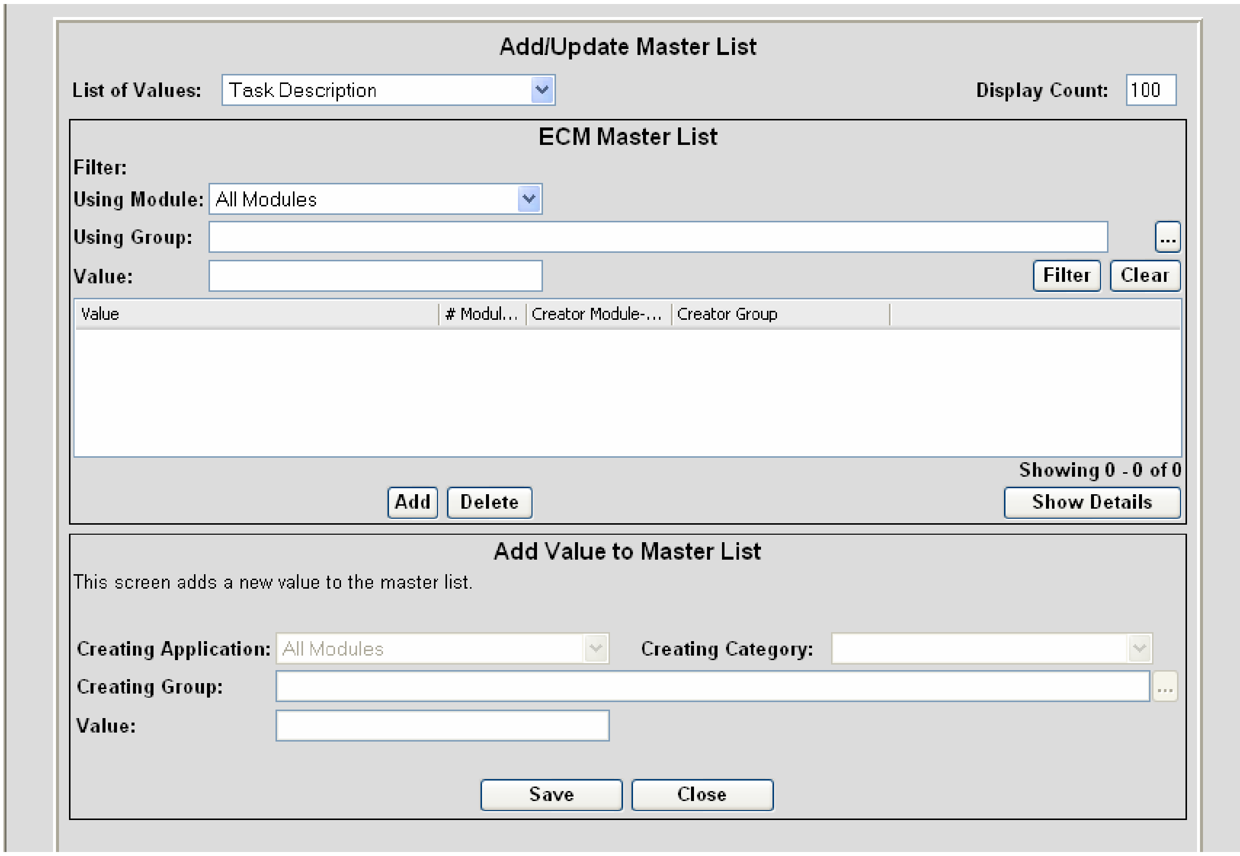


Figure 72: List of Values (Add/Update Master List)

Select the List of Values to be edited (Task Description, in this example).

Click the Filter Button on the Edit Master list screen to display the current values.

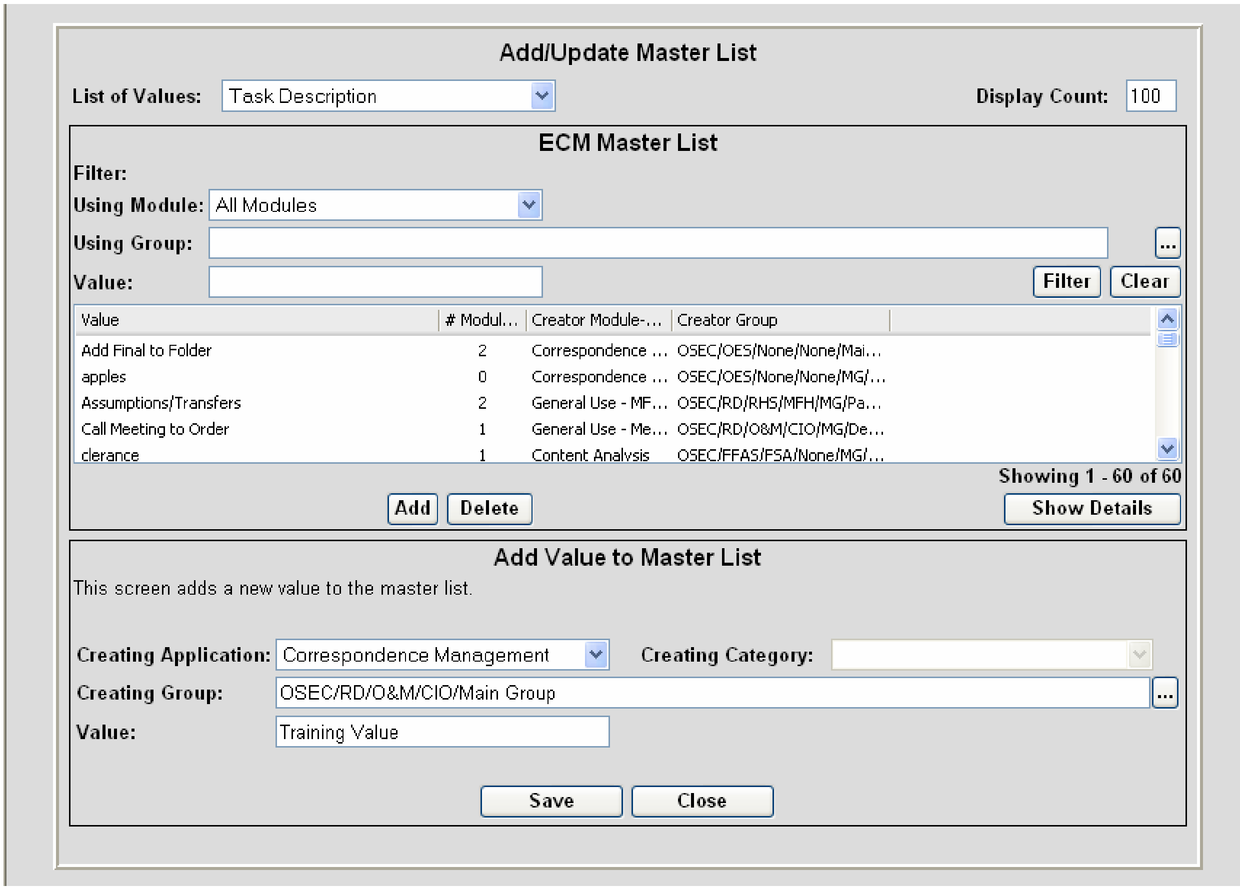


Figure 73: List of Values (Add New Value to Master List)

Click the **ADD** Button to enable the fields on the lower half of the screen.

In the **Add Value to Master List** panel, select and populate **Creating Application**, **Creating Category** (if new value and if for use within General Use Module), and **Creating Group**. Then enter the new list item in the **Value** box. (Please note that the maximum length of a list item is 25 characters.) In the example above, the added list item is "Training Value."

Once the new item has been entered, click the **SAVE** button. If no other values are to be added, click the **CLOSE** button.

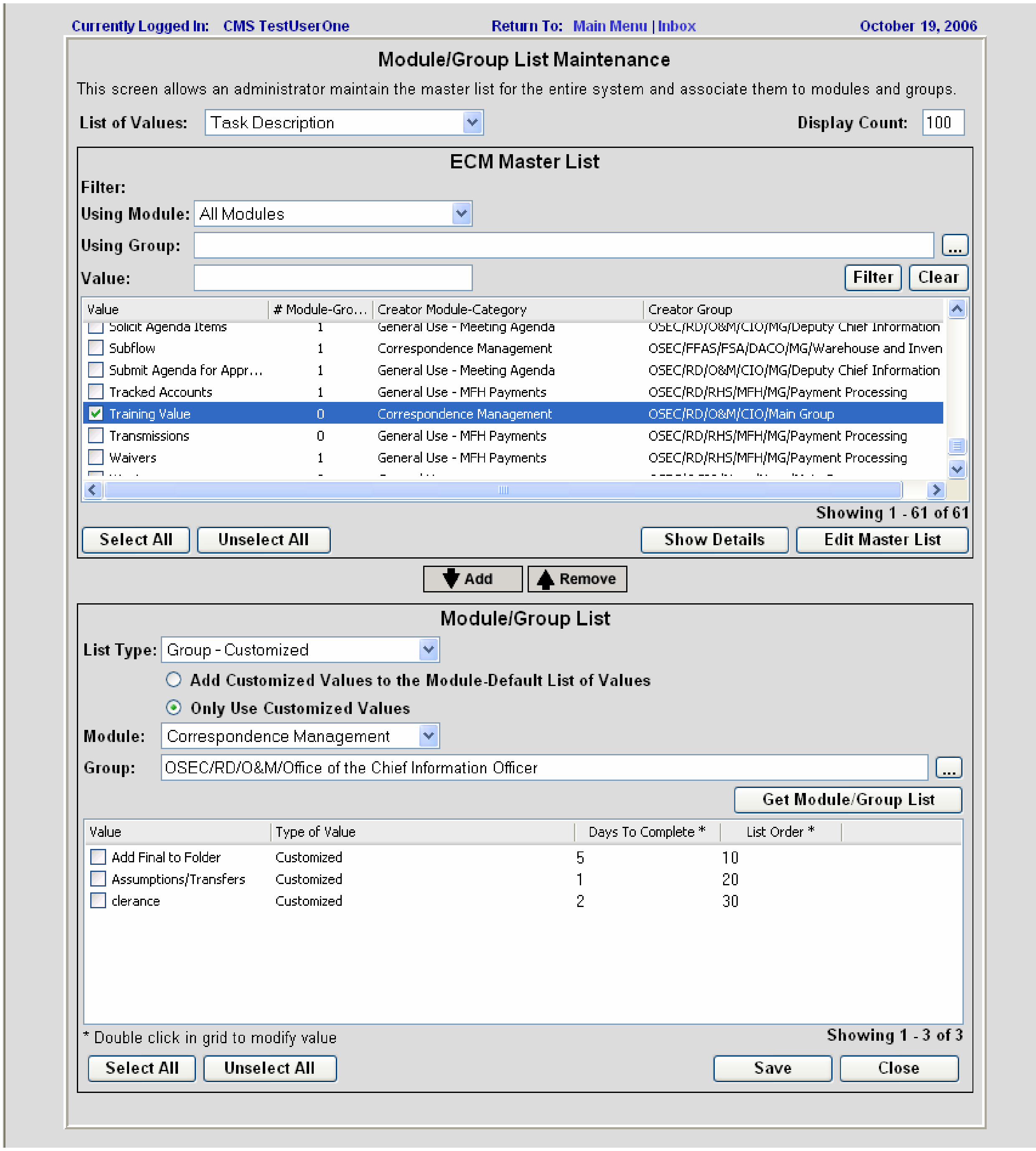


Figure 74: List of Values (Module/Group Maintenance Screen with New Master List Value)

From the Module/Group List Maintenance Screen, refresh the list by clicking the **ECM Master List** FILTER button. The new value, Training Value, is now displayed in the Master List. The new Training Value can now be selected and added to the selected Customized List of Values.

5. Using and Managing Processing Codes

A processing code can be applied to any ECM folder. Processing codes allow ECM users to identify and group similar ECM folders. In most business processes, the processing code is associated with the principal document in the folder.

A powerful feature of ECM is the capability to link a particular processing code with a default workflow. When such a processing code is added to an ECM folder, the default workflow is automatically added to the folder from the ECM workflow library. This feature can simplify folder management and significantly reduce data entry. In the future, we expect to provide the capability to also link default security templates to processing codes.

Processing Code Key Features:

- Processing codes are used to identify and group similar folders (or documents).
- Processing codes may include up to six alpha or numeric characters in any combination.
- Any folder may use a processing code from any list of processing codes in the application.
- Users may identify (in their personal profile) a default set of processing codes for folders they create.

Group administrators, agency group administrators, module administrators, and application administrators can create and modify processing codes. (Group administrators must have administrative privileges for the target group to which the processing codes are attached, or administrative privileges for a parent group of the target group.)

Managing Processing Codes

To create, modify, or delete a processing code, click on the “Processing Code” item on the Administration Menu.

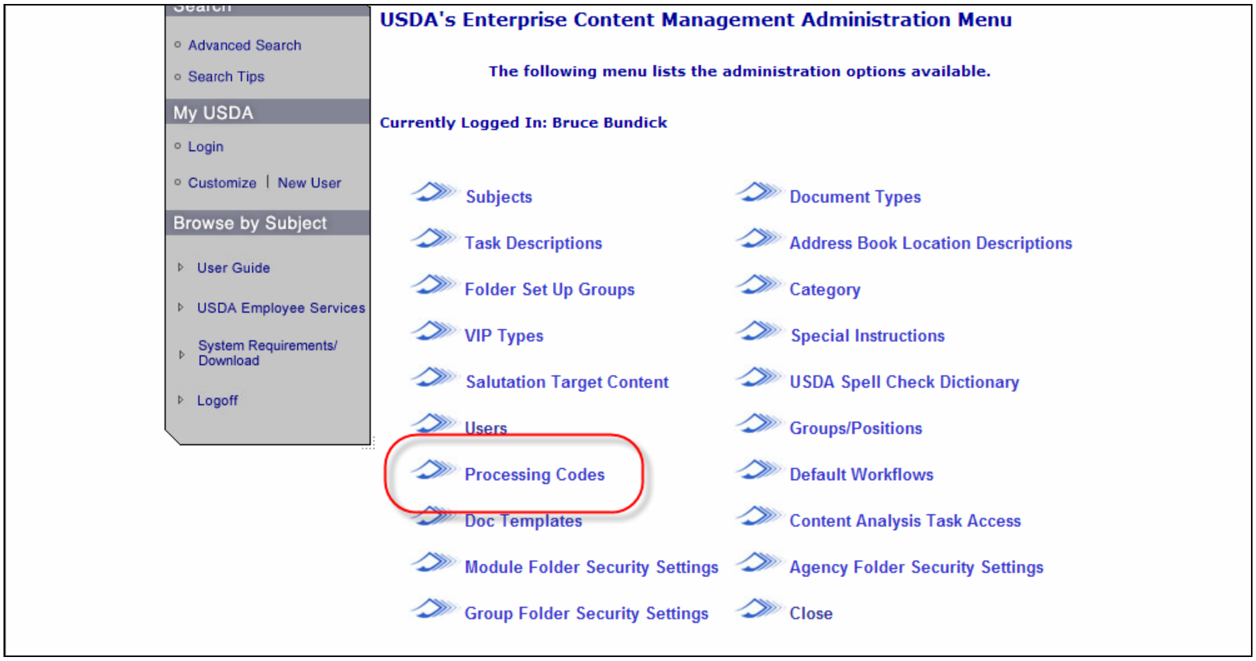


Figure 75: Administration Menu (Processing Codes Link)

Selecting the Processing Codes menu item opens the Processing Code Maintenance screen and allows the administrator to add or delete processing codes or modify their descriptions.

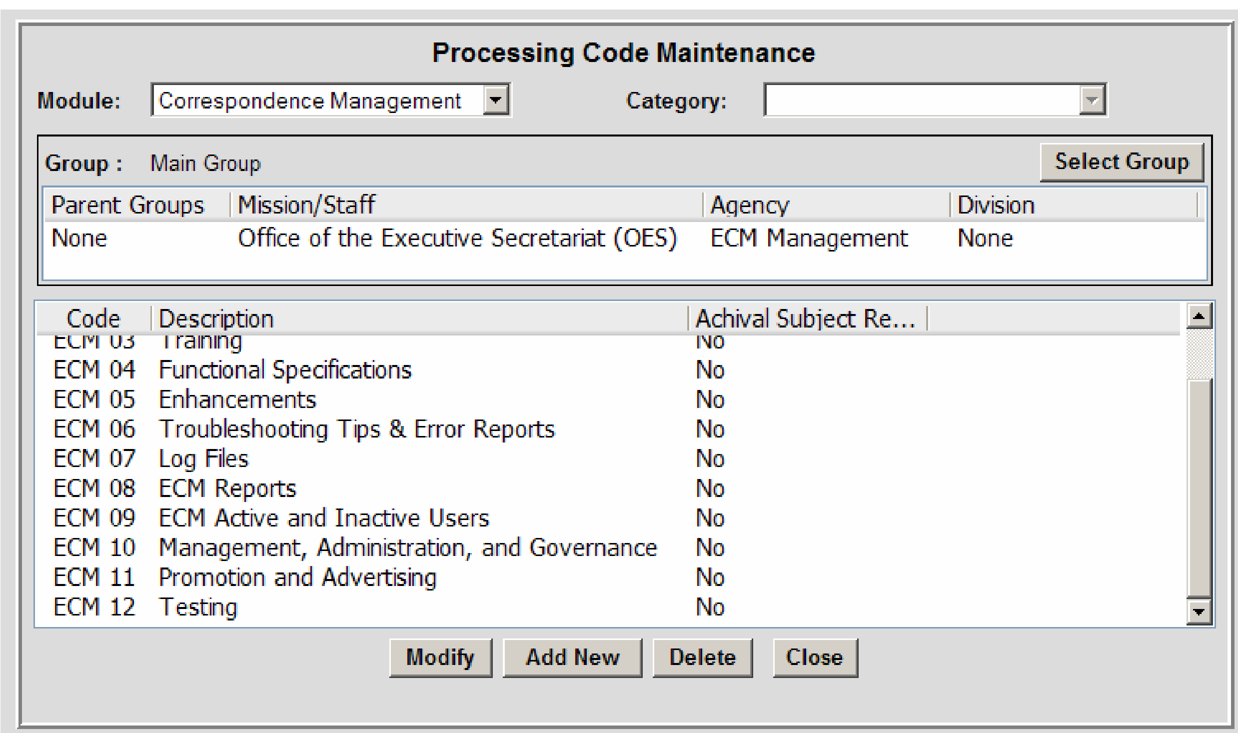


Figure 76: Processing Code Maintenance Screen

Processing codes are linked to a specific ECM group, and they are typically used by a particular Mission Area/Office, Agency, Division or group.

Note: If the processing codes you wish to view or edit are not displayed, use the “Select Group” button to open the standard ECM Select Group List View screen. Navigate to and select the group whose processing codes you want to view or edit.

Modify Existing Processing Code

To modify an existing processing code, highlight a processing code and click on the <Modify> button.

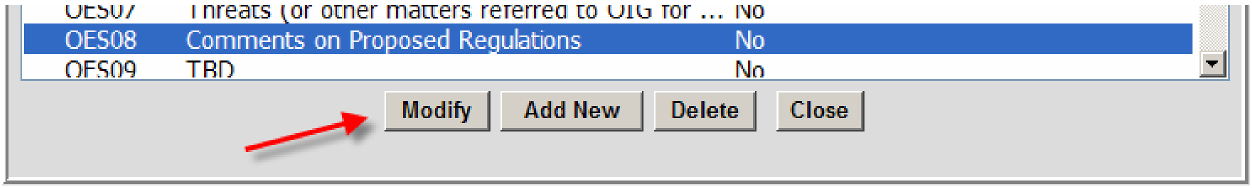


Figure 77: Processing Code (Modify, Add, or Delete Processing Code)

The following administrative console is displayed. Make the changes required and click <Save>.

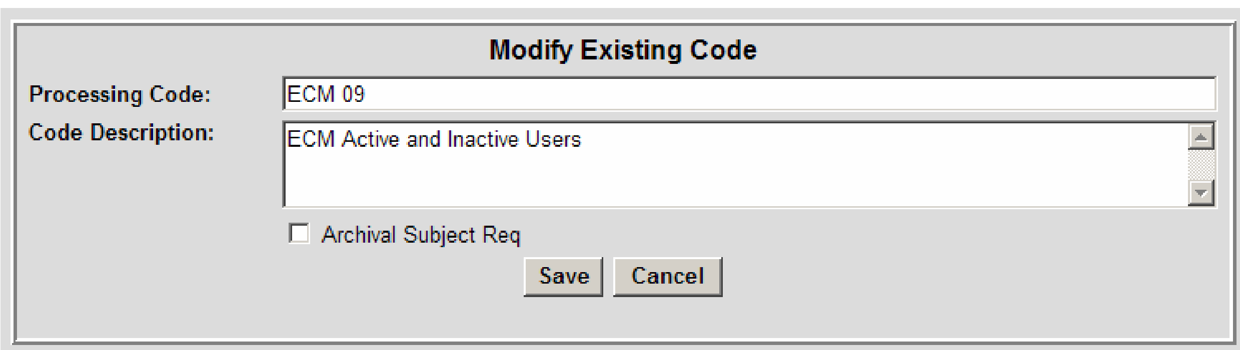


Figure 78: Processing Code (Modify Existing Processing Code)

Create a New Processing Code

To create a new processing code, click on the <Add New> button.

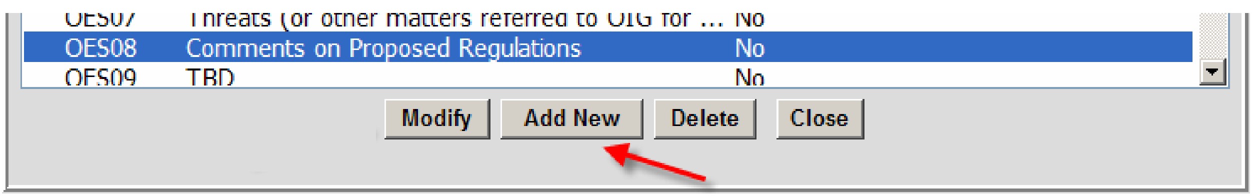


Figure 79: Processing Code (Add New Processing Code)

The following administrative console is displayed. Add a processing code and a code description. If your business practice requires that an archival subject be defined for the class of documents represented by the processing code, check the box, <Archival Subject Req.>. When the required information has been entered, click <Save>.

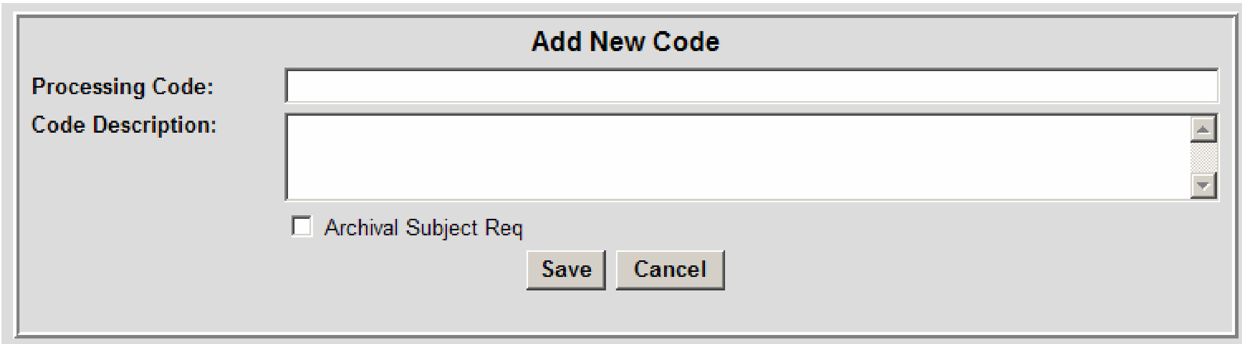


Figure 80: Processing Code (Add New Code)

Delete a Processing Code

To delete a processing code, select and highlight the code to be deleted, and then click on the <Delete> button.

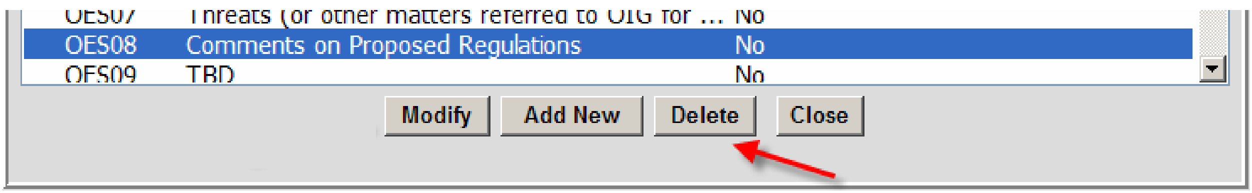


Figure 81: Processing Code (Delete Processing Code)

The following warning message is displayed. To delete the code, click <Yes>. To retain the code, click <No>.

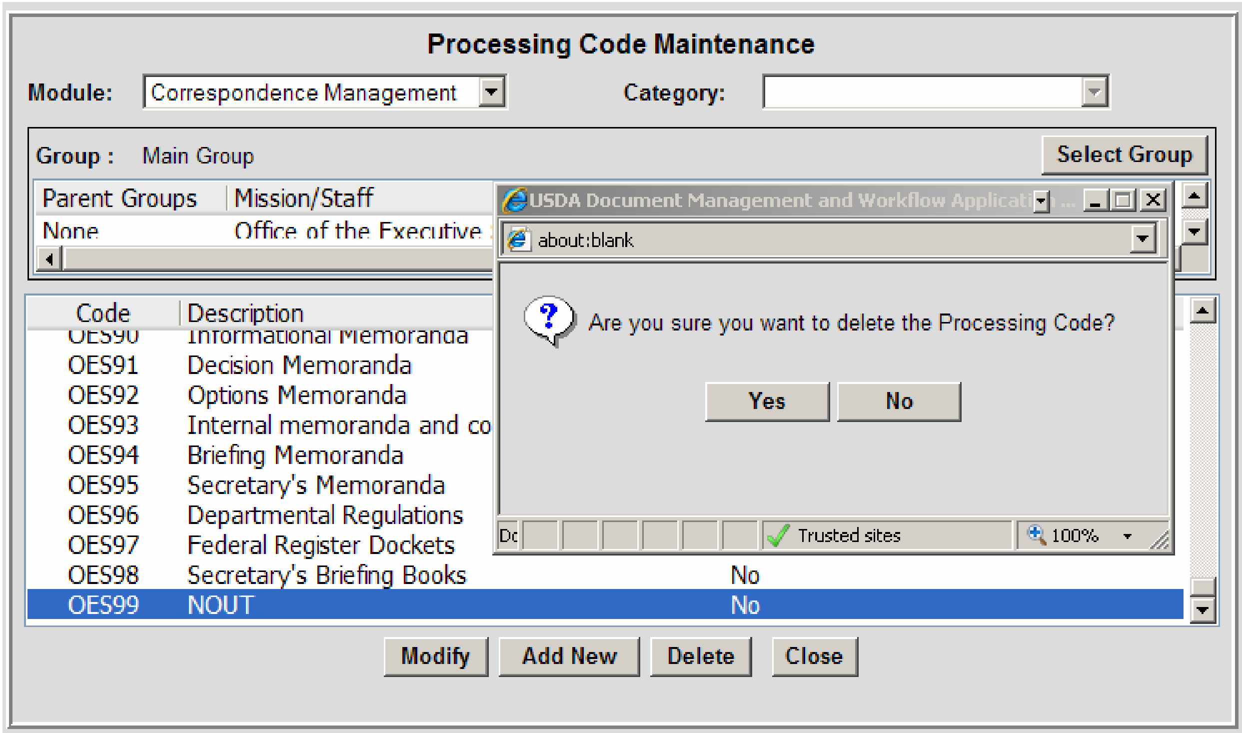


Figure 82: Processing Code (Confirm Delete Processing Code)

Associate a Processing Code with a Workflow Template

A most useful feature of ECM is its ability to associate a standard workflow with a processing code. When the processing code is added to an ECM folder, the associated workflow template is copied from the workflow library and inserted on the folder.

To associate a default workflow with a particular processing code, select the **DEFAULT WORKFLOW** link from the ECM Administration Submenu.

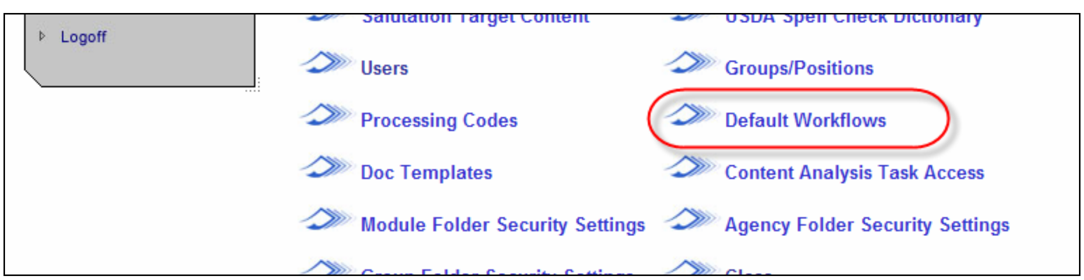


Figure 83: Administration Submenu—Default Workflow Link

The Default Workflow Maintenance screen is displayed.

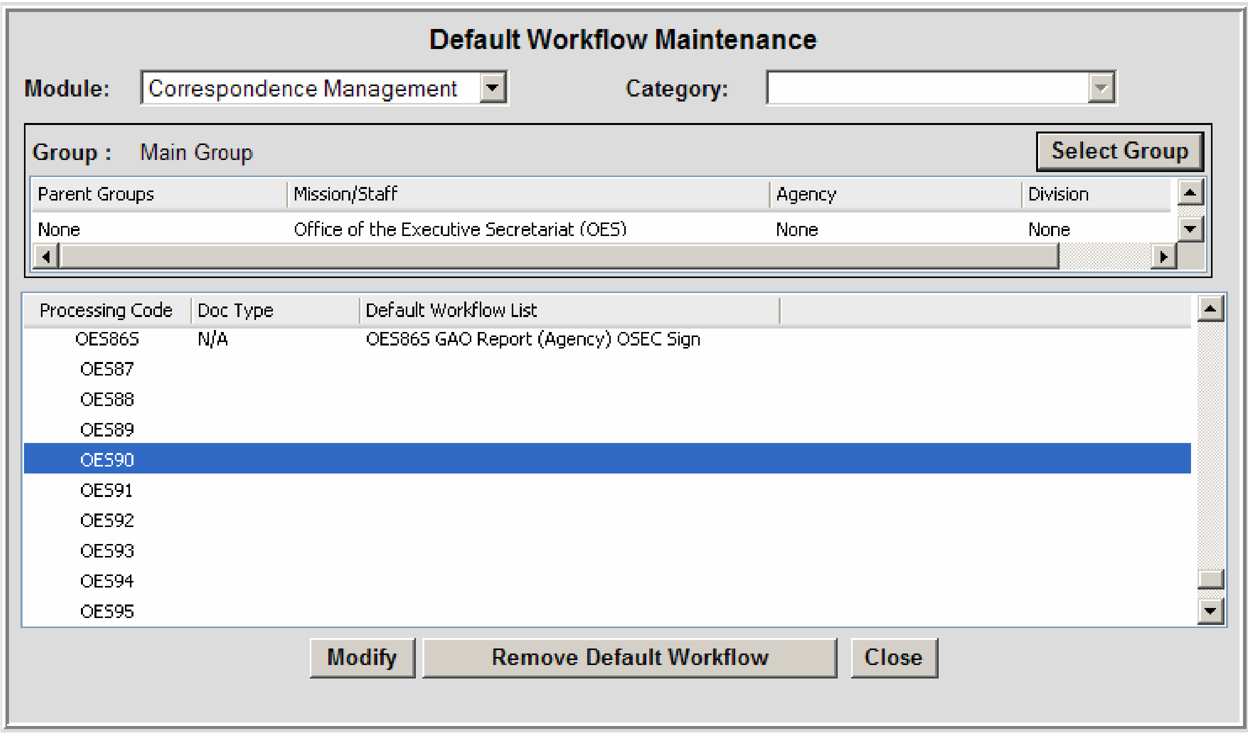


Figure 84: Default Workflow Maintenance Screen (Select Processing Code)

On the Default Workflow Maintenance screen, click the **SELECT GROUP** button to locate and select the group that "owns" the list of processing codes you wish to modify. When the group is selected, the list of all processing codes associated with that group will be displayed.

Select the processing code you wish to link to a default workflow.

Click on the **MODIFY** button. The Modify Default Workflow screen is displayed.

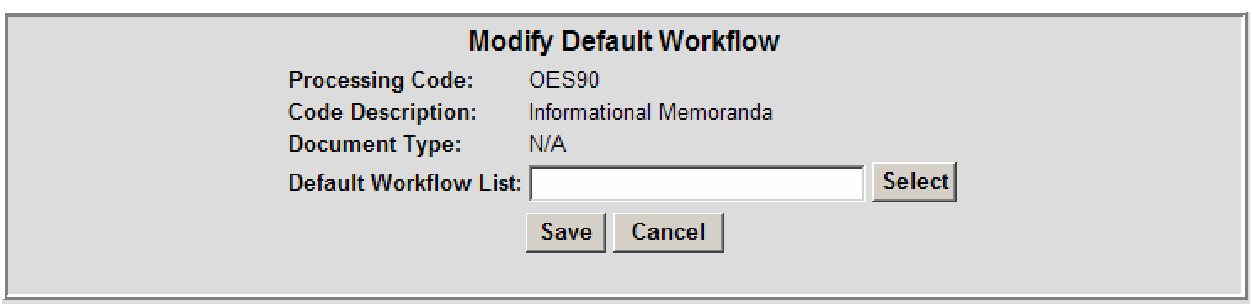


Figure 85: Default Workflow Maintenance (Modify Default Workflow)

Click the **SELECT** button to open the workflow template library.

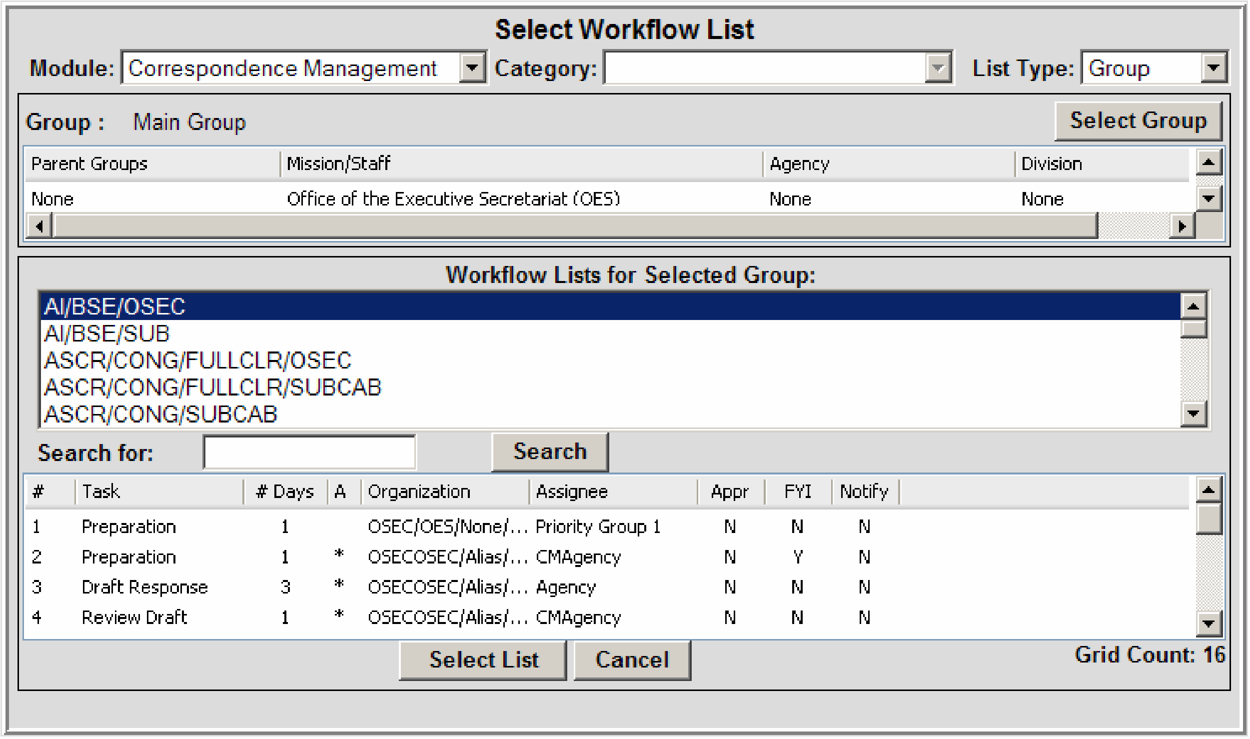


Figure 86: Default Workflow Maintenance (Select Workflow List)

Use the Select Group button to navigate to and select the group that owns the workflow list you want to associate with your processing code. When that group is selected, its Workflow Lists will be displayed.

The center panel on the screen displays the names of the lists associated with the selected group. The bottom panel displays the actual workflow list for the workflow selected in the center panel.

When the appropriate workflow has been located and highlighted in the center panel, click the **SELECT LIST** at the bottom of the screen.

The selected workflow list is now associated with the processing code.

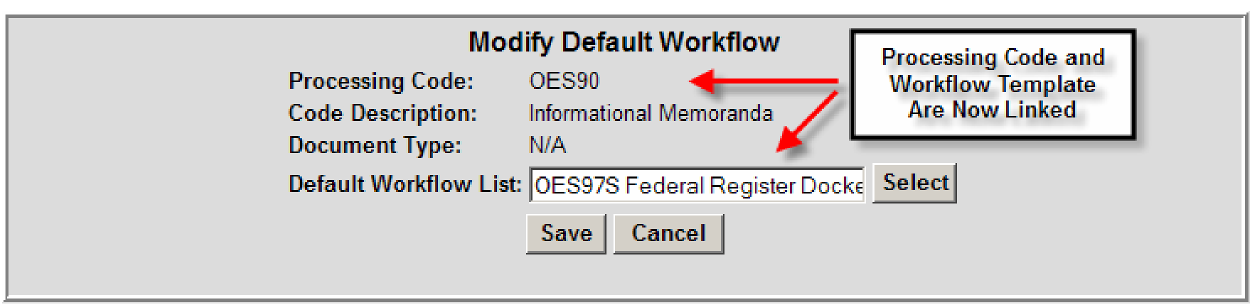


Figure 87: Modify Default Workflow (Processing Code and Workflow Associated)

Click **SAVE** to complete the action. Click **CANCEL** to abandon the association or to start over.

6. ECM Security

Security Overview

The ECM application secures folders and documents based on the role of the user with respect to the folder and the agency to which the user belongs. The security model provides folder owners with great control over the security of ECM folders and documents.

Each folder has a Folder Owner. The Folder Owner may be a user or a group. When the Folder Owner is a group, all members of that group have Folder Owner privileges for the folder.

The Folder Owner has privileges to add or change any folder field values. The folder fields are on the top panel of the folder (see the folder example on the following page). Folder fields provide descriptive information about the folder.

The Folder Owner can also add or change the main workflow and add or change documents stored in the folder. The Folder Owner can perform these operations at any time while the folder status is "Active." When the folder status is "Closed or Archived," no further changes can be made.

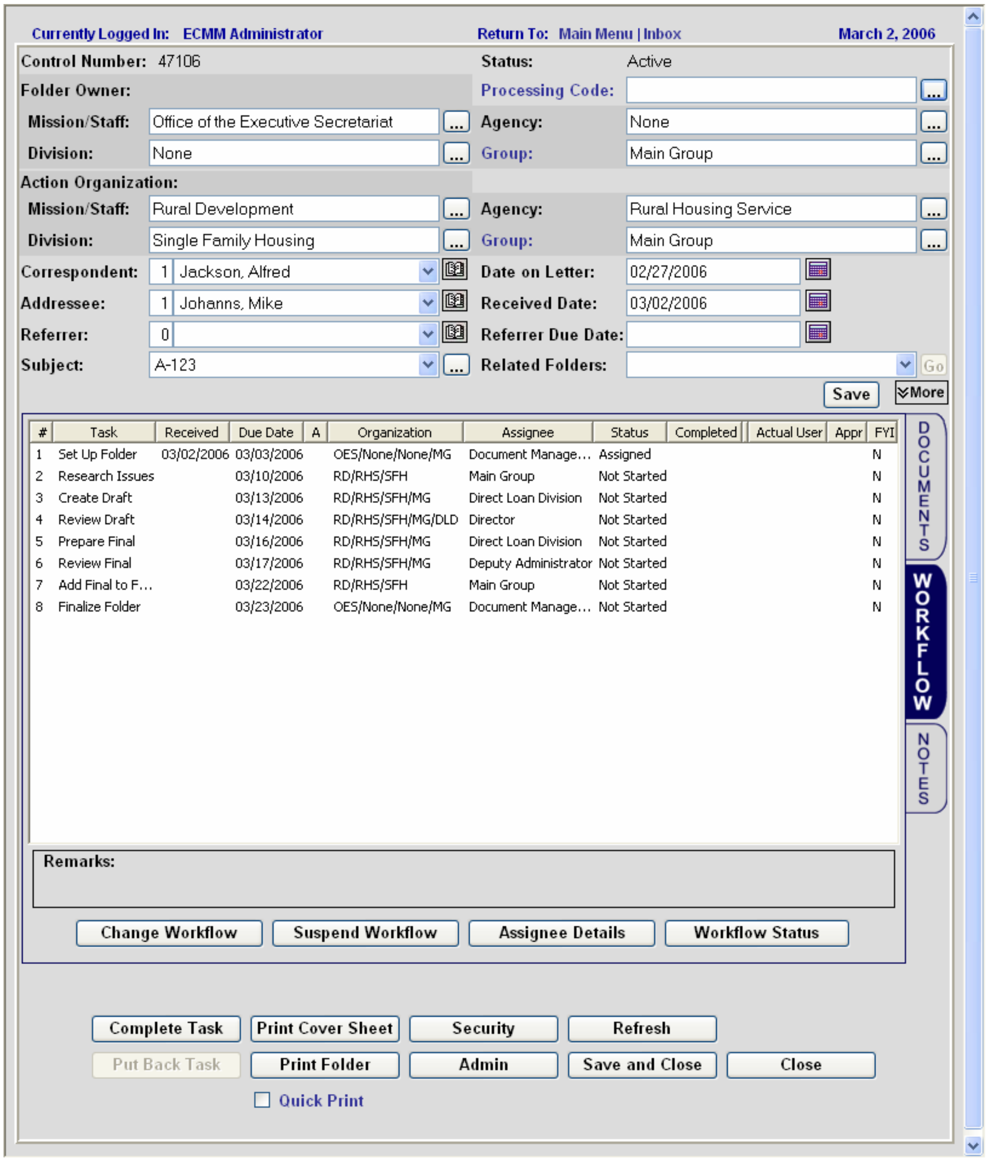


Figure 88: Security (Example of Opened Folder)

The range of security settings available to folder owners can be set for an ECM module or established at any point within the organizational hierarchy. Unless prohibited by the available security settings, a folder-owning group may set access privileges for Application Administrators, Module Administrators, Agency Group Administrators, and Group Administrators. Each class of administrator may be granted Folder Owner privileges (View, Edit) or View Only access, or they may be restricted from access. Security screens allow the Folder Owner to set the specific privileges for each type of administrator.

When a user is working on a current workflow task for a folder, the user has privileges to make certain changes to the folder. The current task assignee may change the folder's Action Organization Division and/or Group. The task assignee may also select additional subjects for the folder but cannot change subjects selected by the Folder Owner. The current task assignee may add a subflow for his or her task in the workflow but may not change the main workflow. The task assignee may add or change documents stored in the folder.

Other users or groups in the organization may be granted view-only privileges to a folder. View-only privileges include the ability to add notes to a folder. The Folder Owner grants or denies privileges to users in the Folder Owner's Organization and the Action Organization. Privileges can be granted at a broad level such as all users in the Rural Development agency or at a lower level such as all users in the Centralized Servicing Center of Rural Development. The Folder Owner can also grant privileges to a specific user or group by adding them to an access control list for the folder.

Within USDA, certain users are designated as privileged users. Privileged users have the rights to view all folders within their organization (their organizational level and all organizations below it). The rights of privileged users to view a folder can be maintained by the Folder Owner (within limits set for the module).

Folder Security Settings

The Folder Security screen allows a Folder Owner to set security levels for a folder. The range of security levels that may be granted is set on a module by module basis by an Application or Module Administrator.

Each agency may also set the minimum and maximum security settings for all of its folders (based on the Folder Owner organization). An Agency Group Administrator has the privileges to define the Agency Folder Security settings. When Agency Folder Security settings are defined, they override the minimum and maximum settings defined for the module. However, Agency Folder Security Settings may not be less restrictive than the minimum and maximum security settings defined for the Module or for a higher-level organization.

To change the security for a folder, the Folder Owner clicks the <Security> button. The Folder Security screen is displayed as shown below.

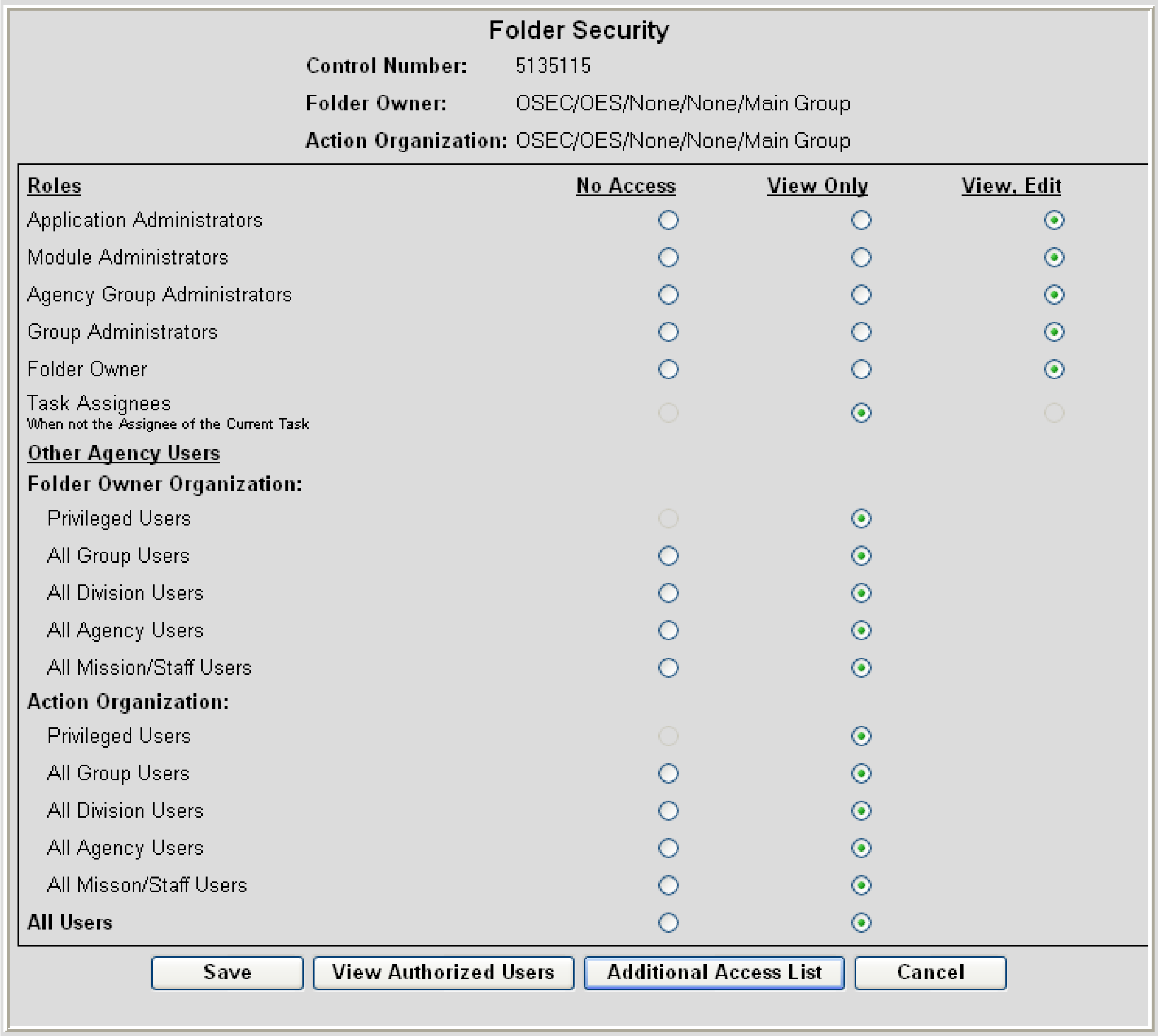


Figure 89: Folder Security Maintenance

The screen is displayed with the default security selections. The Folder Owner can make changes to the default security within the minimum and maximum settings established for the Module or Agency. Grayed-out radio buttons are options that were outside the minimum and maximum settings established at the Module or a higher group level.

The Roles section defines security based on a user's role with respect to the folder. The roles are Application Administrator, Module Administrator, Agency Group Administrator, Group Administrator Folder Owner, and Task Assignees (when not on the current task).

The available choices for Roles are No Access, View-only, or View/Edit. With View, Edit privileges, Administrators may perform all of the functions that can be performed by the Folder Owner. These were described in the Overview section. Assignees with View, Edit privileges can make changes to the folder even when they aren't working the current task. Assignees with View Only privileges can make changes only when they are the assignee of the current task.

The lower section defines privileges for Other Agency Users. This section describes the privileges for users who do not have a specified role for the folder. Privileges granted are based on a user's relationship to the Folder Owner Organization and the Action Organization shown on the folder. Privileges for these "Other Agency Users" can be set to View Only access or No Access.

Privileged users are those executive-level users who have been identified as having privileges to view folders throughout their organization. Only a security officer may designate a user as privileged. The security officer also designates the user's organization, which determines the top level of access. Privileged users have access to all folders at the granted organization (anchor point) and all organizations below it. However, the Folder Owner can override this access by setting Privileged Users to "No Access." The module settings could define a range that prevents a Folder Owner from restricting access.

In the screen example above, users in the same Mission/Staff and Agency of the Folder Owner Organization on the folder will have View Only access to this folder. All users in the same Mission/Staff and Agency of the Action Organization on the folder will also have View Only access to this folder. Other users in the organization will have No Access to this folder.

When a broader access level is granted, the narrower definitions are automatically granted and the radio buttons will show this. For example, when the Folder Owner sets Mission/Staff, Agency to View Only:

- Mission/Staff, Agency, Division Users is set to View Only, and
- Mission/Staff, Agency, Division, Group Users is set to View Only.

If All Users is set to View Only, all other designations are set to View Only.

To see a list of users who are authorized to access the folder, the Folder Owner clicks the <View Authorized Users> button. The following screen is displayed.

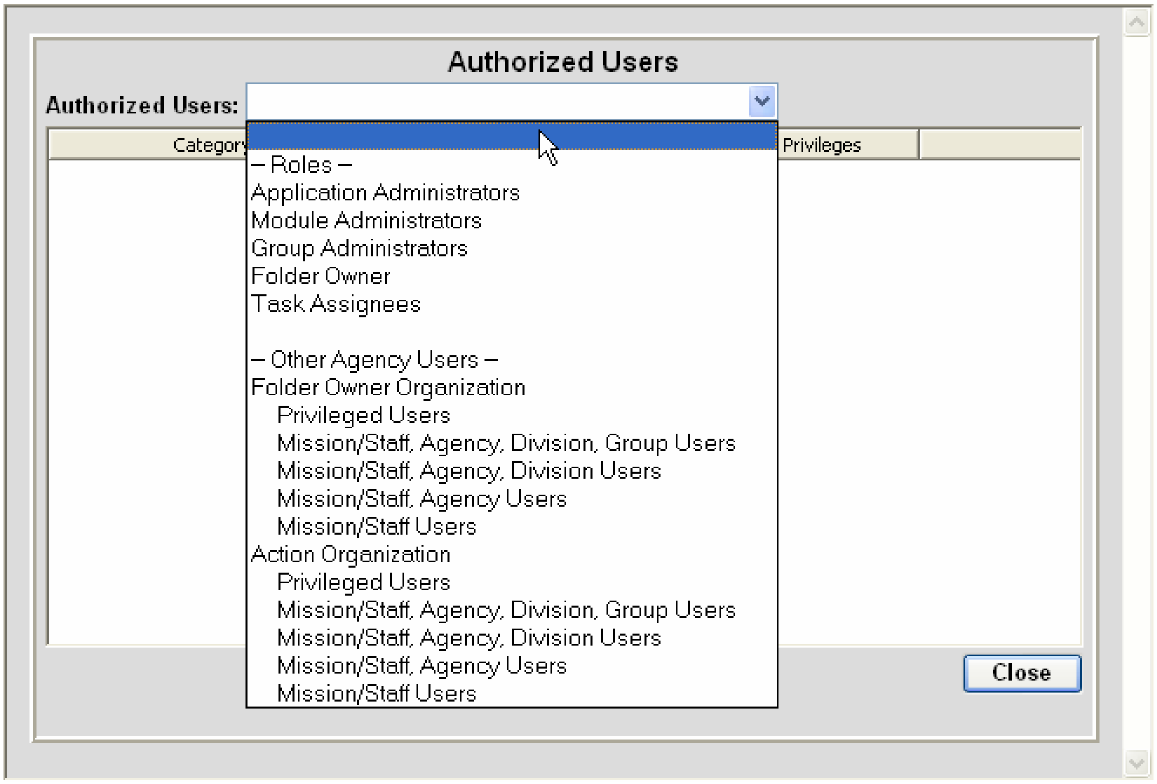


Figure 90: Select Authorized Users Category to View

This screen allows the user to select the individual folder roles and view the authorized users for that role (as shown below). A category of All Users with access can also be selected.

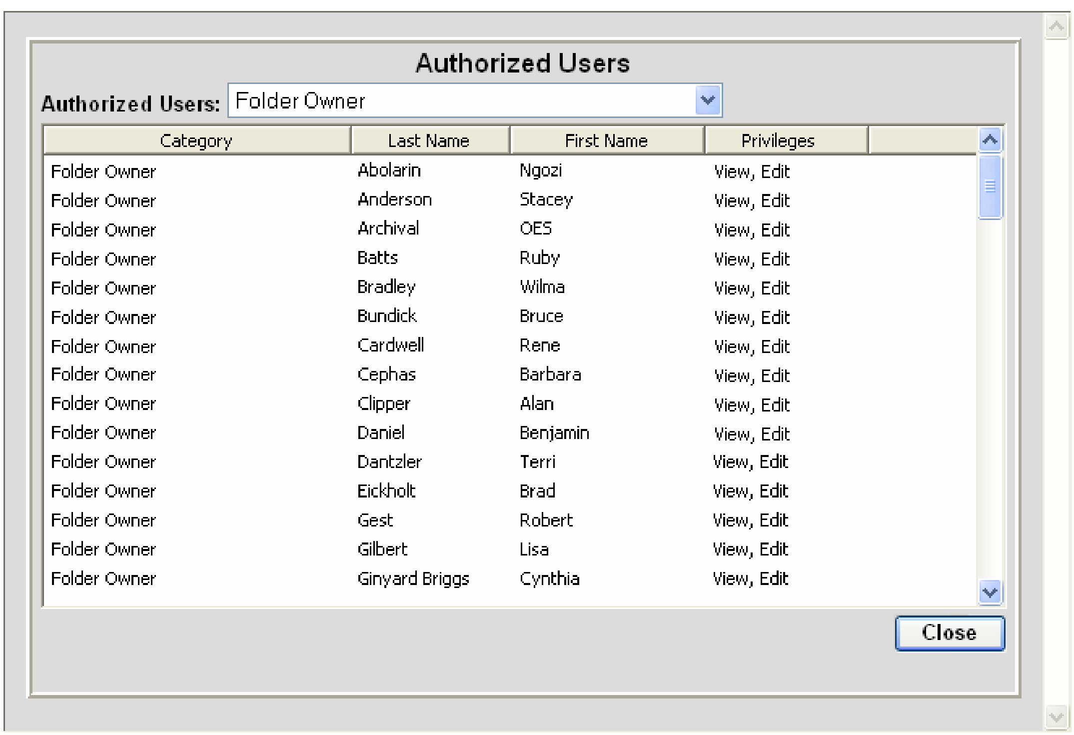


Figure 91: List of Authorized Folder Owners for Folder

The Folder Owner (or administrator with Folder Owner privileges) may explicitly grant access to the folder for a specific user or group. The Folder Owner clicks the <Additional Access List> button. The Additional Access List screen is displayed.

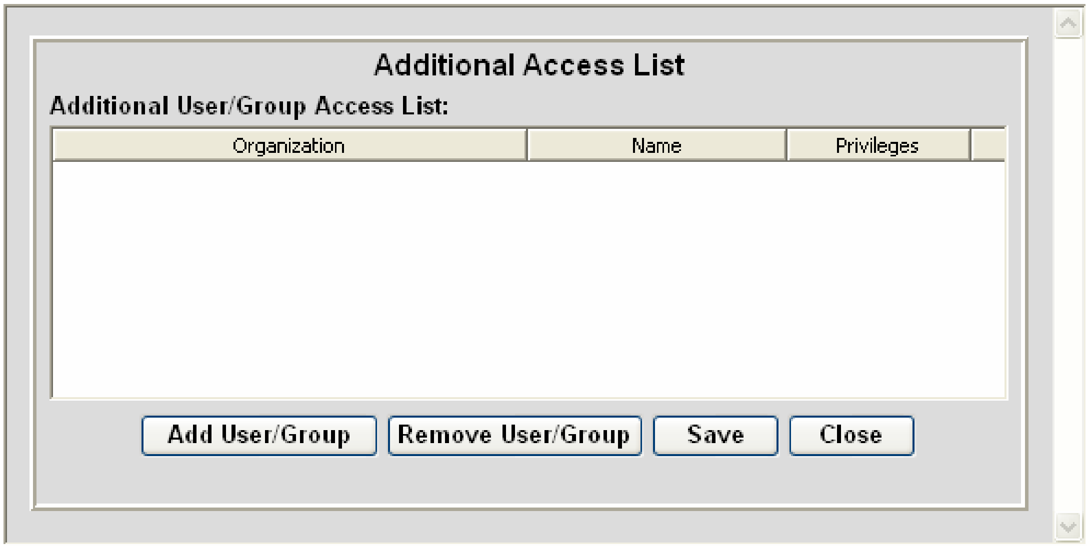


Figure 92: Additional Access List

To add a user or group, the Folder Owner clicks the <Add User/Group> button.

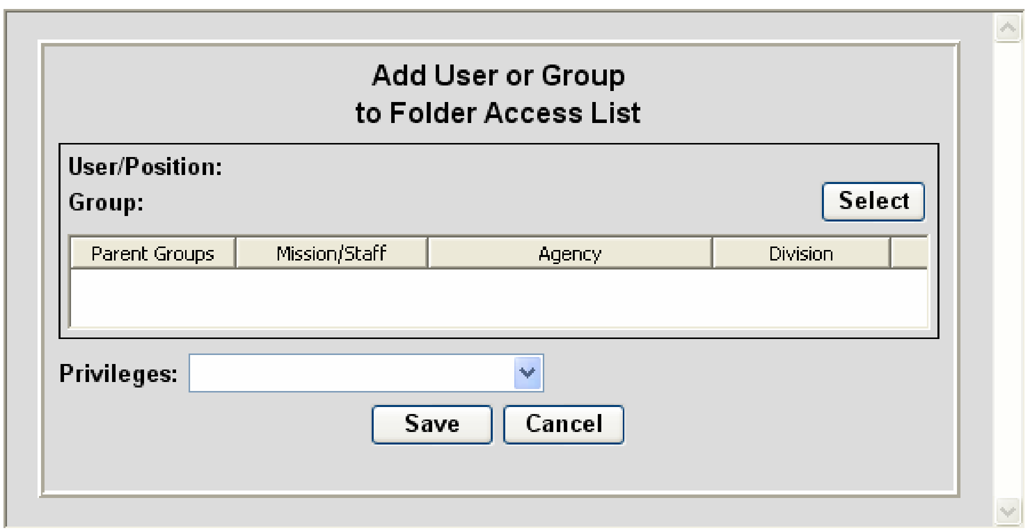


Figure 93: Add User or Group to Folder Access List

To select a user or group, the Folder Owner clicks the <Select> button. The Select Group/Position/User screen is displayed.

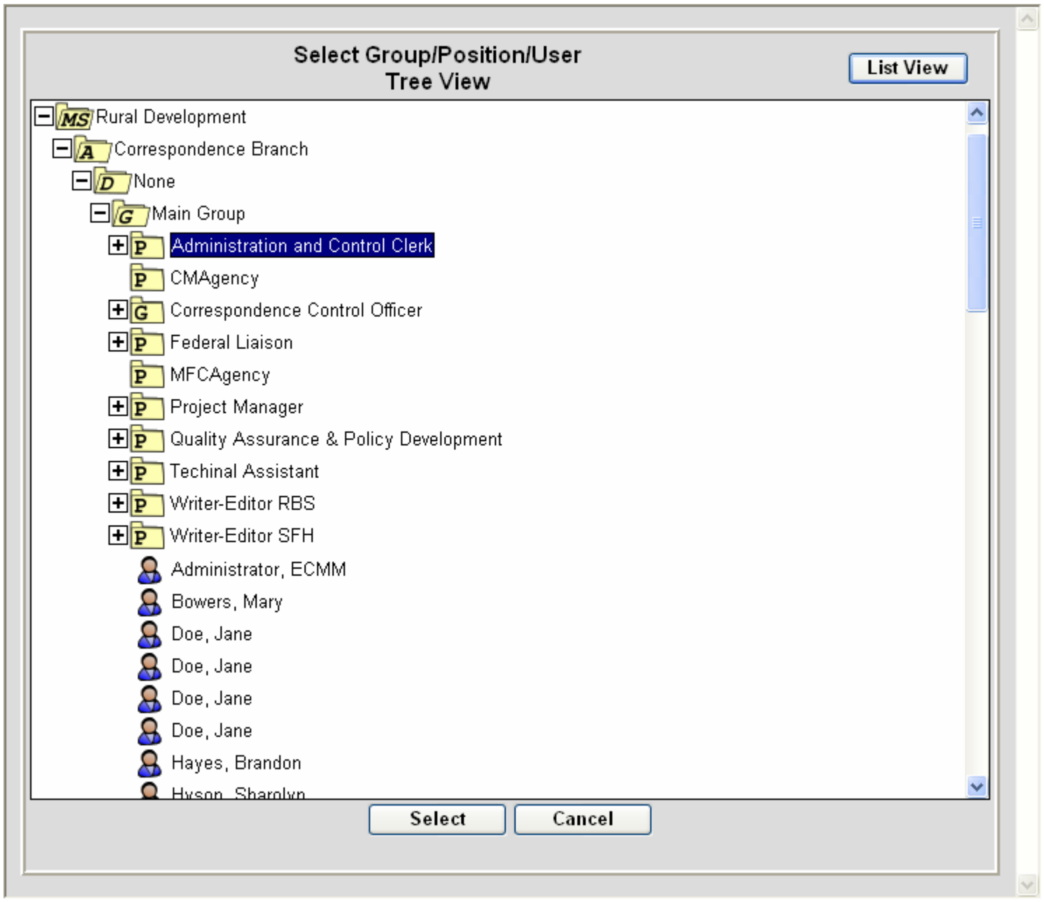


Figure 94: Select Group/Position/User

The Folder Owner makes a selection and clicks the <Select> button. The Add User or Group screen is re-displayed with the new selection.

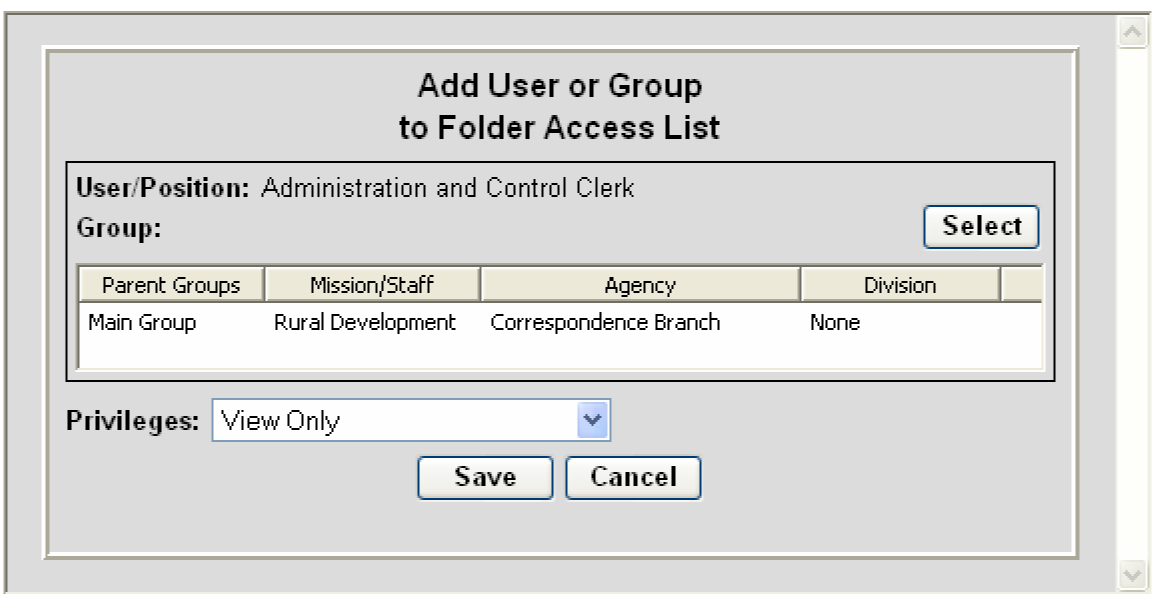


Figure 95: Add User or Group to Folder Access List - Position Selected

The Folder Owner selects the Privilege level to be granted and clicks the <Save> button.

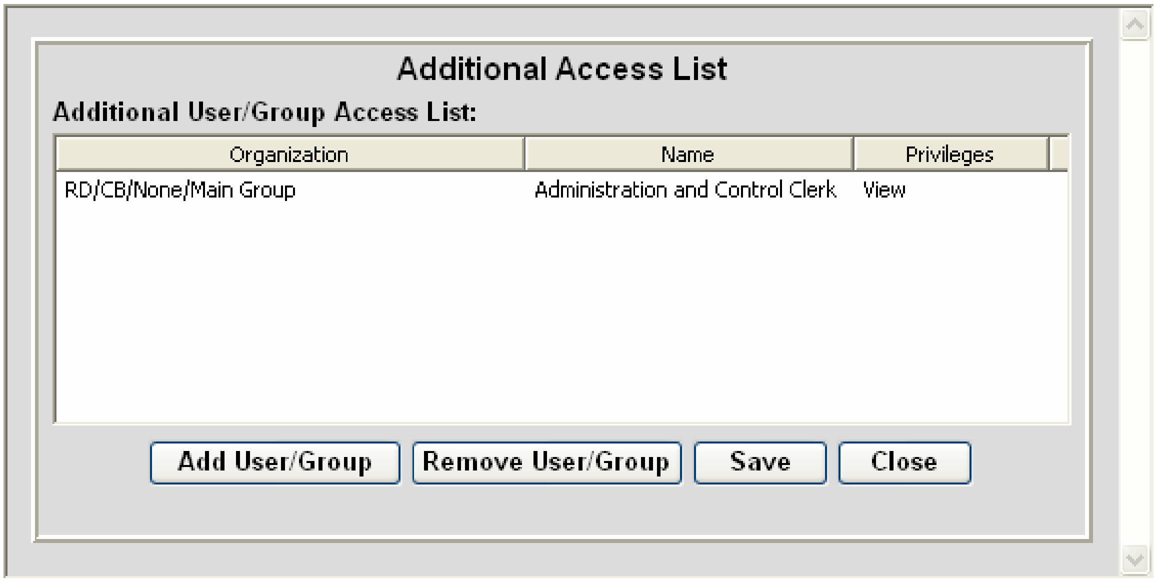


Figure 96: Additional Users Access List

To save the changes, the Folder Owner clicks the <Save> button. The Administration and Control Clerk position is added to the Folder Access List. Any user associated with that position would have View Only privileges for this folder.

Module Folder Security Settings

As mentioned above, the minimum and maximum access privileges for each category of user are set by an Application or Module Administrator for each ECM Module. The following Module Security screen is accessible from the ECM Administration menu.

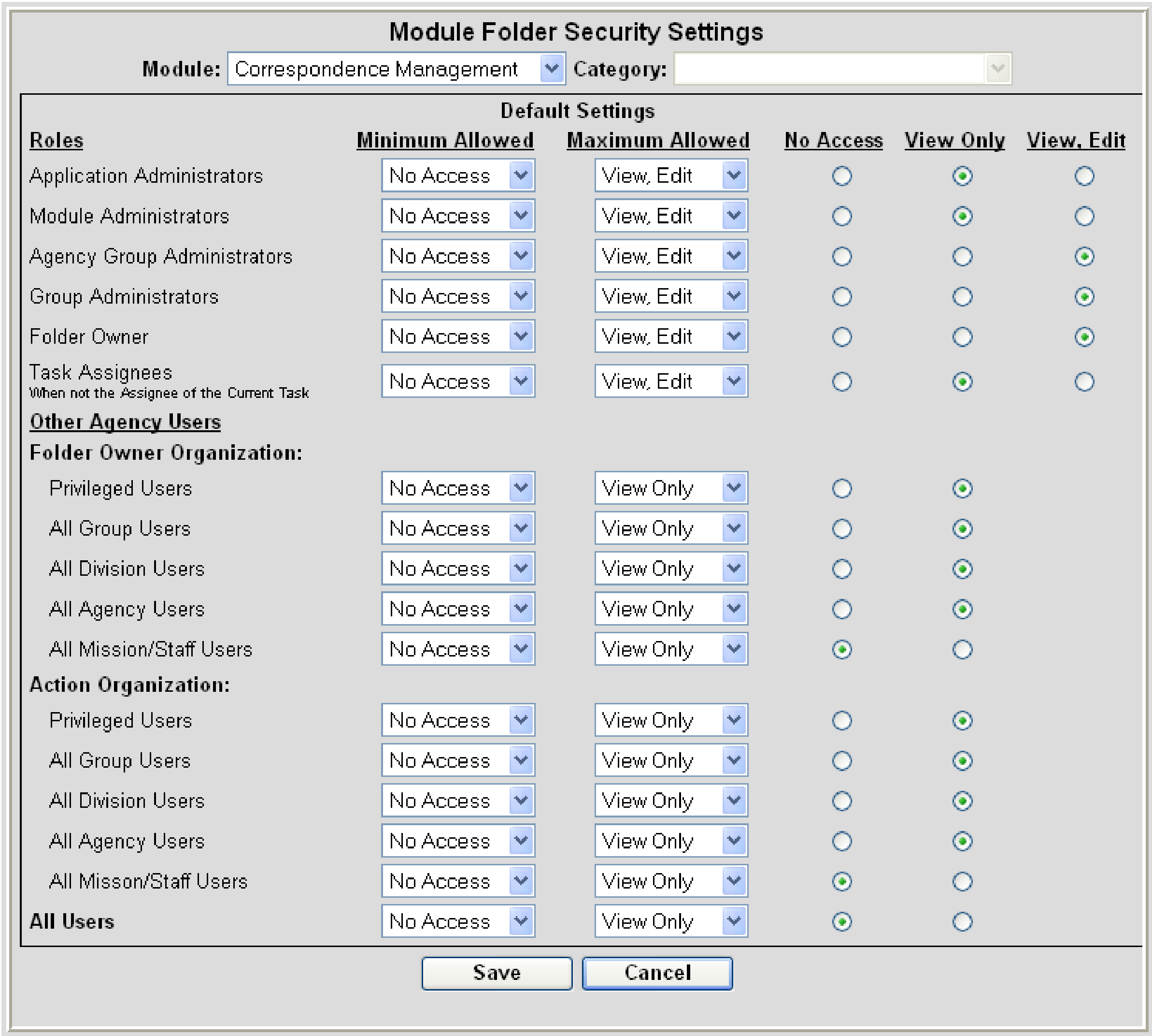


Figure 97: Folder Security—Correspondence Management Module Default Settings

An Application or Module Administrator can change the “Minimum Allowed” and “Maximum Allowed” privileges for users within the module. These limits cannot be exceeded in setting the Agency and Group Security Default Settings.

In the example above, the minimum access that can be set in the Correspondence Module for all users is “No Access,” which means that a user cannot view or edit the folder.

The maximum access that can be granted to users with a Role as Application, Module, Agency Group and Group Administrator, and Folder Owner and Task Assignees in a folder is “View, Edit.” “View, Edit’ privileges allow the user to enter the folder, view and modify folder data fields, and perform workflow functions and tasks.

The minimum access that can be set for all other agency users within the Folder Owner Organization and the Action Organization is “No Access.” The maximum access is “View Only.” The “View Only” privilege allows the user to view the folder and the data it contains but not to change it.

The figure below displays the folder security screen based on the maximum, minimum, and default security settings at the module above. This is the screen that would be available to the Folder Owner and all users with View, Edit access to the folder.

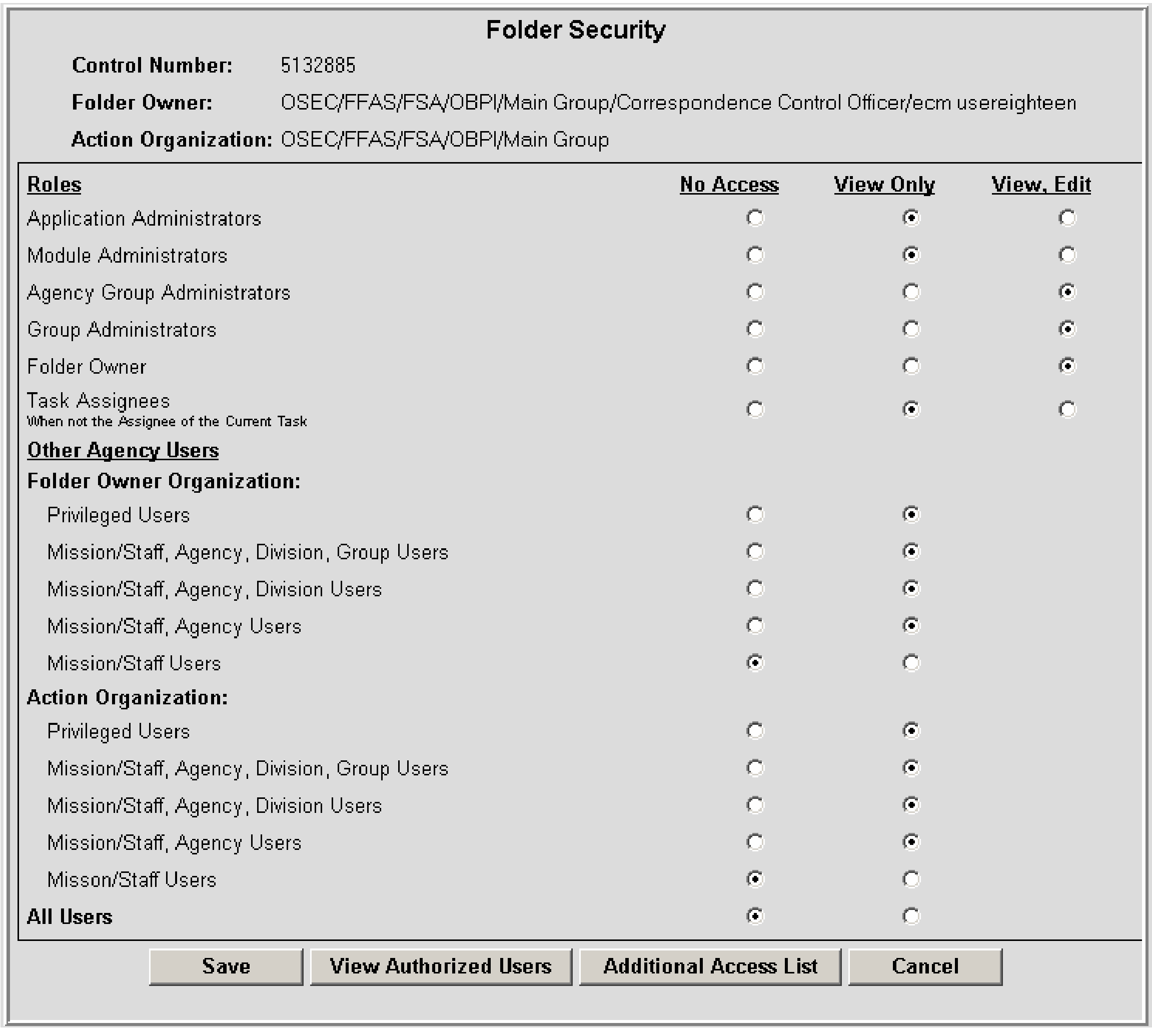
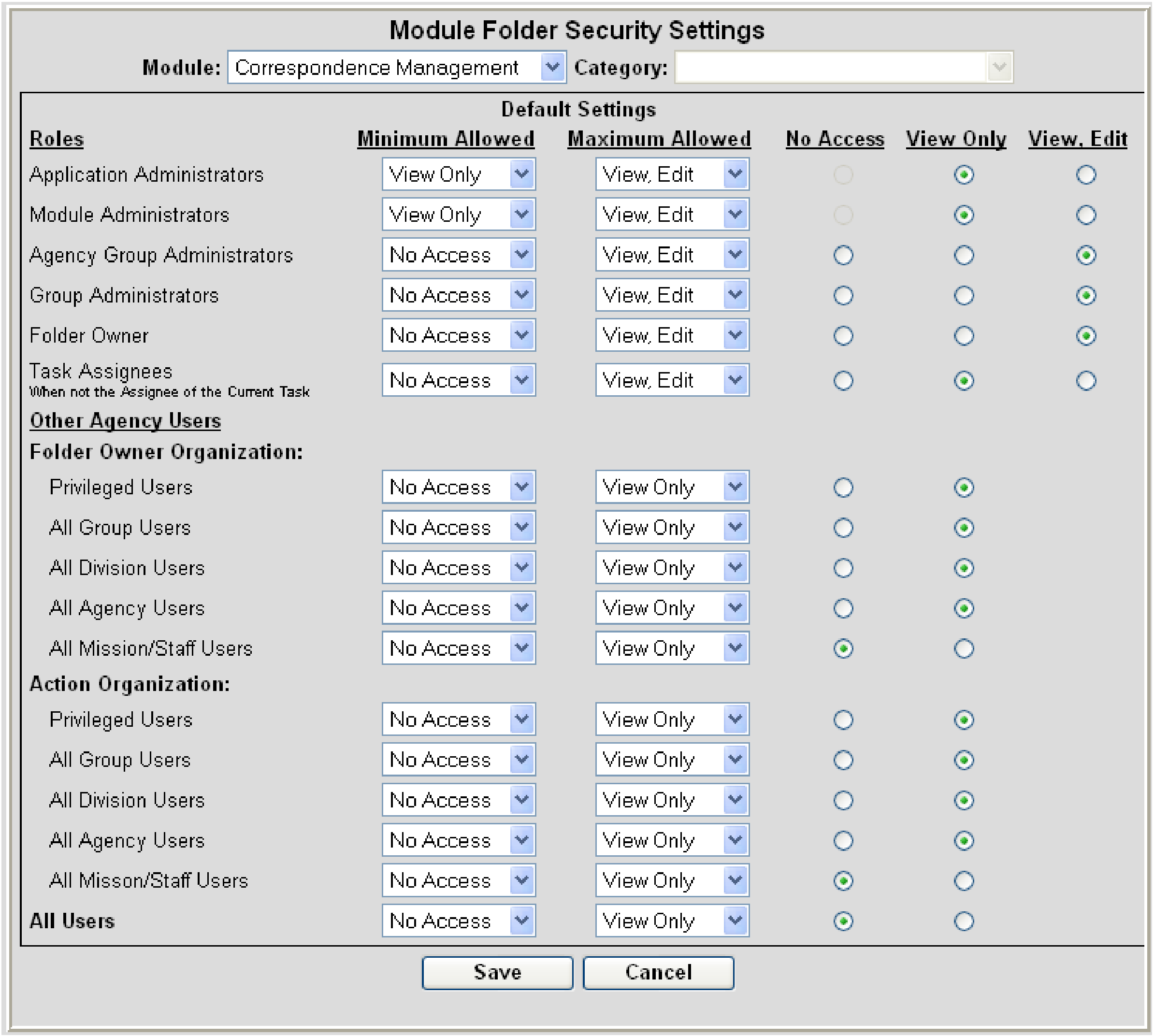


Figure 98: Folder Security—Folder with the Current Default Settings

In the example displayed in the figure above, all of the radio buttons are available and active. The default module settings, from which this screen is derived, permit the full range of available options for each user role or user group.

If the Application or Module Administrator sets the ‘Minimum Allowed’ access default for Application Administrators and Module Administrators at ‘View Only,’ the radio buttons under the ‘No Access’ heading are grayed out and cannot be selected. Thus, the folder owner cannot deny at least View access to Application and Module Administrators. This condition is displayed in the figure below.



Module Folder Security Settings

Module: Correspondence Management Category:

Roles	Default Settings: Minimum Allowed	Default Settings: Maximum Allowed	No Access	View Only	View, Edit
Application Administrators	View Only	View, Edit	( )	(•)	( )
Module Administrators	View Only	View, Edit	( )	(•)	( )
Agency Group Administrators	No Access	View, Edit	( )	( )	(•)
Group Administrators	No Access	View, Edit	( )	( )	(•)
Folder Owner	No Access	View, Edit	( )	( )	(•)
Task Assignees When not the Assignee of the Current Task	No Access	View, Edit	( )	(•)	( )
Other Agency Users					
Folder Owner Organization:					
Privileged Users	No Access	View Only	( )	(•)	
All Group Users	No Access	View Only	( )	(•)	
All Division Users	No Access	View Only	( )	(•)	
All Agency Users	No Access	View Only	( )	(•)	
All Mission/Staff Users	No Access	View Only	(•)	( )	
Action Organization:					
Privileged Users	No Access	View Only	( )	(•)	
All Group Users	No Access	View Only	( )	(•)	
All Division Users	No Access	View Only	( )	(•)	
All Agency Users	No Access	View Only	( )	(•)	
All Misson/Staff Users	No Access	View Only	(•)	( )	
All Users	No Access	View Only	(•)	( )	

Save Cancel

Figure 99: Module Folder Security Settings

Agency Group Security Settings

Agency Group Administrators set the defaults for their Agency within the parameters set at the Module level.

In the example above, the Module settings have been modified. As a result, Agency and Agency Group Administrators do not have the option of changing the “Minimum Allowed” to “No Access” for Application and Module Administrators.

In the example below, an Agency Administrator for FFAS/FSA can choose only “View Only” or “View, Edit” as minimum allowed default settings within the Agency for Application and Module Administrators. This is also true for any subgroups.

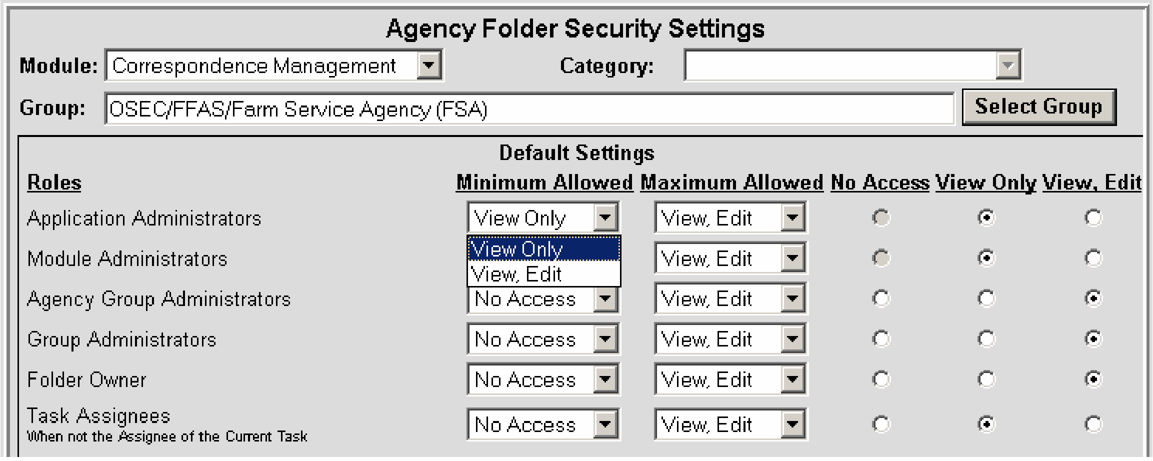


Figure 100: Folder Security—Agency Folder Security Settings Based on Module Settings

The figure below displays the Default Settings as they are expressed at the Folder Level based on higher-level setting making ‘No Access’ unavailable as options for users and administrators.

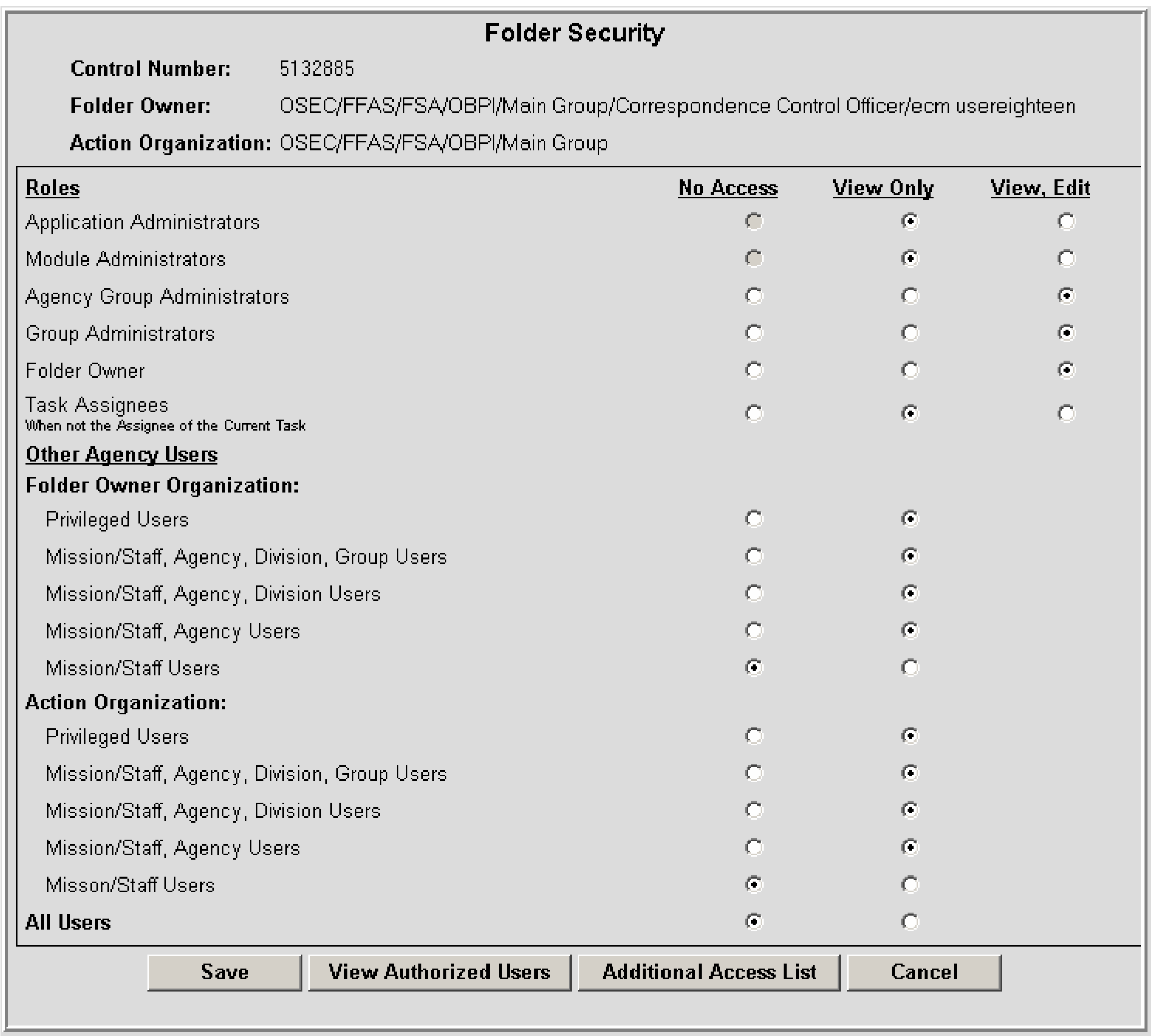
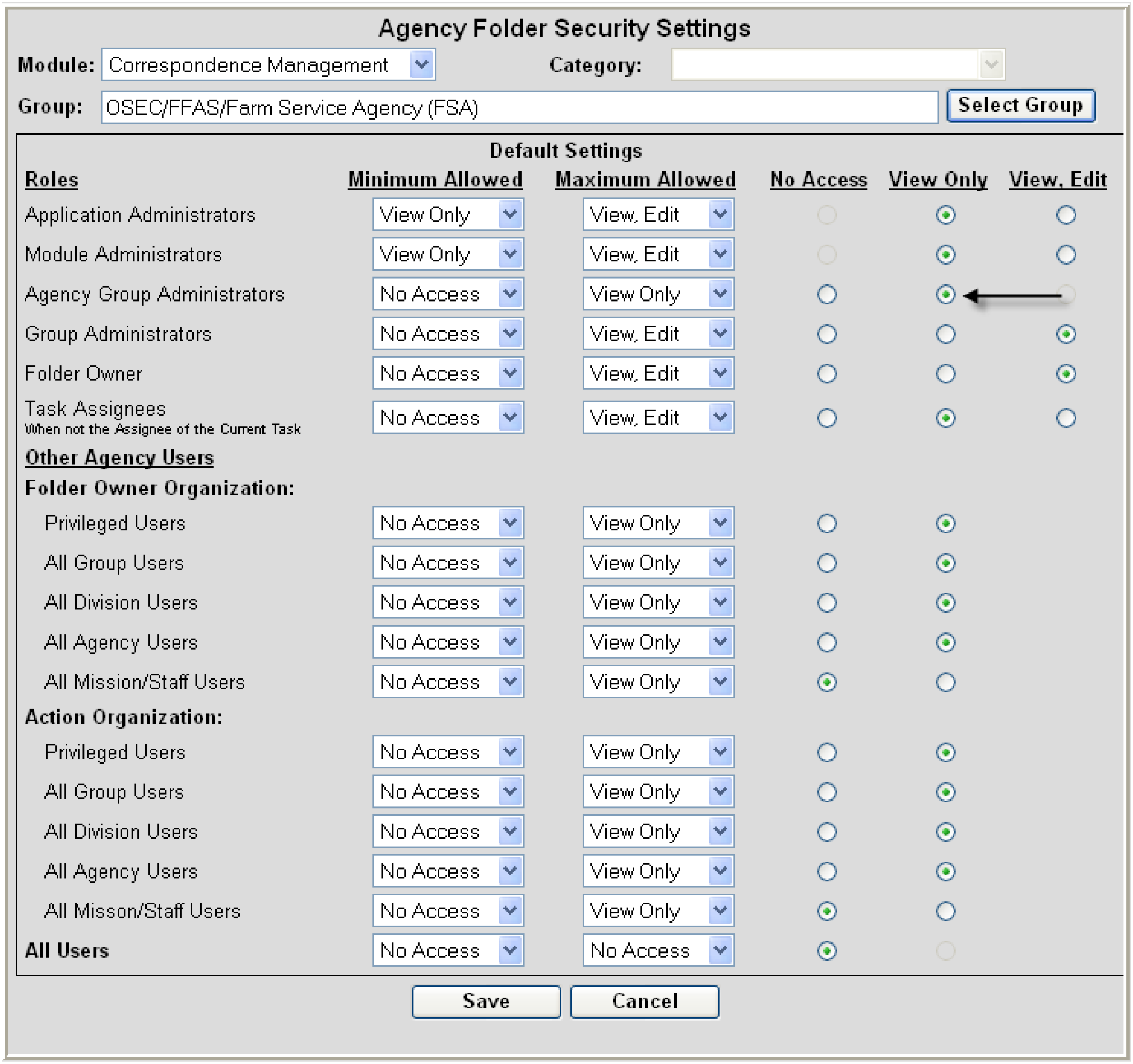


Figure 101: Folder Security—Available Folder Security Settings Based on Module Settings

In the example below, the Agency Group Administrator has modified the “Maximum Allowed” folder access for Group Administrators to “View Only.” Therefore, the “View, Edit” button is grayed out for that role. The grayed out ‘No Access” buttons for Application and Module Administrators reflect limits set at a higher (Module) level. Thus, the options available at the folder level represent the sum of the restrictions made at all higher levels.



Agency Folder Security Settings

Module: Correspondence Management | Category: | Group: OSEC/FFAS/Farm Service Agency (FSA) | Select Group

Default Settings

Roles	Minimum Allowed	Maximum Allowed	No Access	View Only	View, Edit
Application Administrators	View Only	View, Edit			
Module Administrators	View Only	View, Edit			
Agency Group Administrators	No Access	View Only			
Group Administrators	No Access	View, Edit			
Folder Owner	No Access	View, Edit			
Task Assignees When not the Assignee of the Current Task	No Access	View, Edit			
Other Agency Users					
Folder Owner Organization:					
Privileged Users	No Access	View Only			
All Group Users	No Access	View Only			
All Division Users	No Access	View Only			
All Agency Users	No Access	View Only			
All Mission/Staff Users	No Access	View Only			
Action Organization:					
Privileged Users	No Access	View Only			
All Group Users	No Access	View Only			
All Division Users	No Access	View Only			
All Agency Users	No Access	View Only			
All Misson/Staff Users	No Access	View Only			
All Users	No Access	No Access			

Save | Cancel

Figure 102: Agency Folder Security Settings

Group Folder Security Settings

Default security settings may be defined at the group level. Maximum and minimum settings may not be defined at this level. Those settings are those set for parent groups by Application, Module, or Agency Group Administrators. A Group Administrator (or higher level Administrator) with administrative privileges for a group or a parent group can set default security settings for the group. The next three figures display the navigation to the group.

Figure 103: Group Folder Security Settings – Select Group

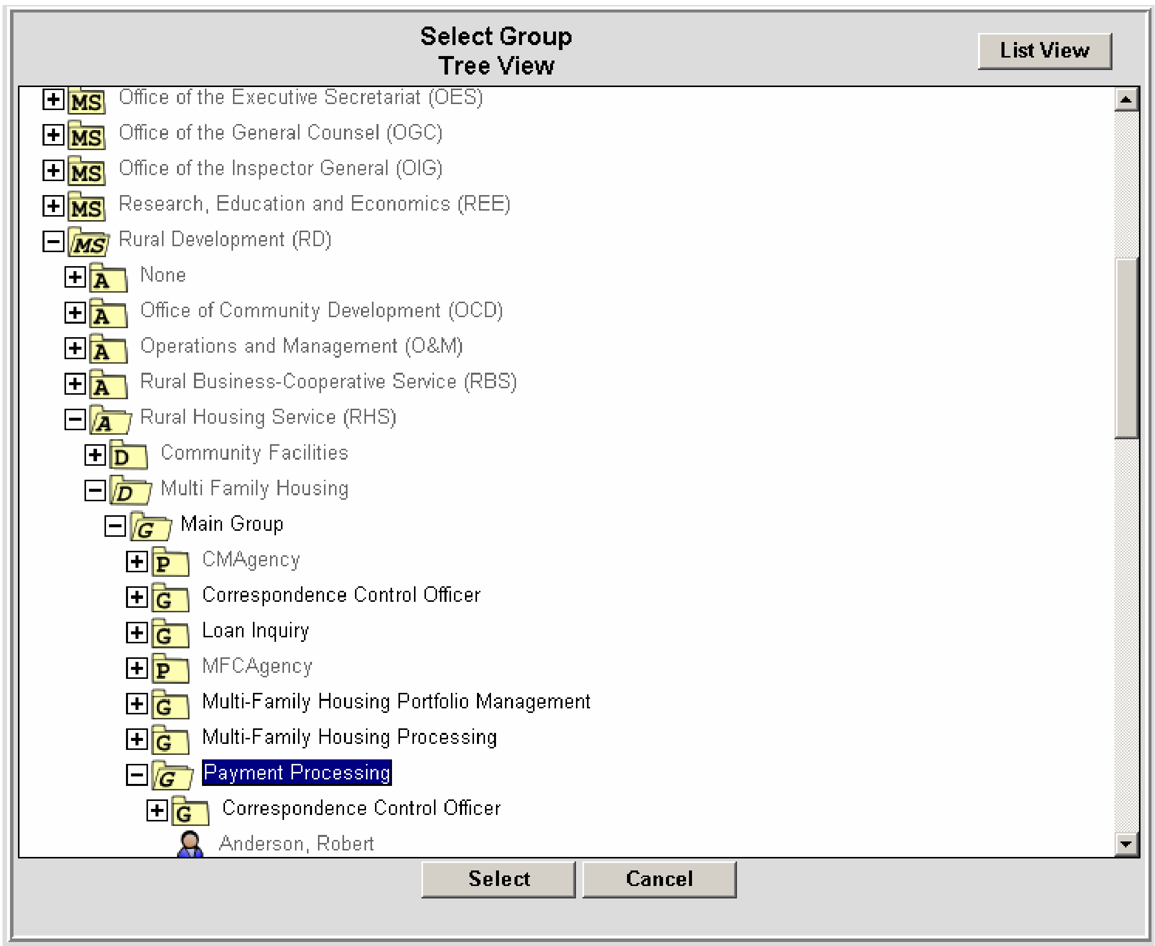


Figure 104: Group Folder Security Settings—Select Group (Tree View)

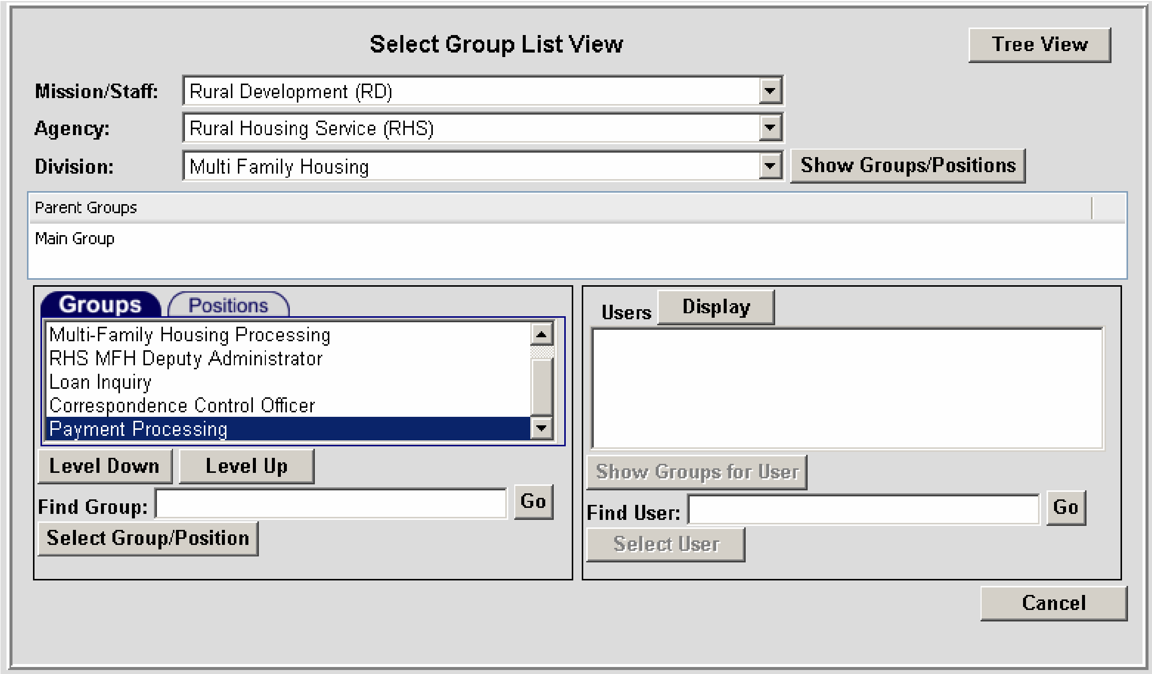


Figure 105: Group Folder Security Settings—Select Group (List View)

In the examples above, the Security defaults are set at the Agency level within the maximum and minimum settings previously established. Note that the drop-down lists of maximum and minimum settings are not available on the Group Folder Security screen.

Therefore, Group Administrators may change the default settings, but they cannot change the range of options available to a Folder Owner within that group.

Access granted to Agency Group Administrators as “View Only.” As a result, a Group Administrator defining Group-level security cannot change the default settings for a particular group to grant “View, Edit” privileges to Agency Group Administrators. This is illustrated below.

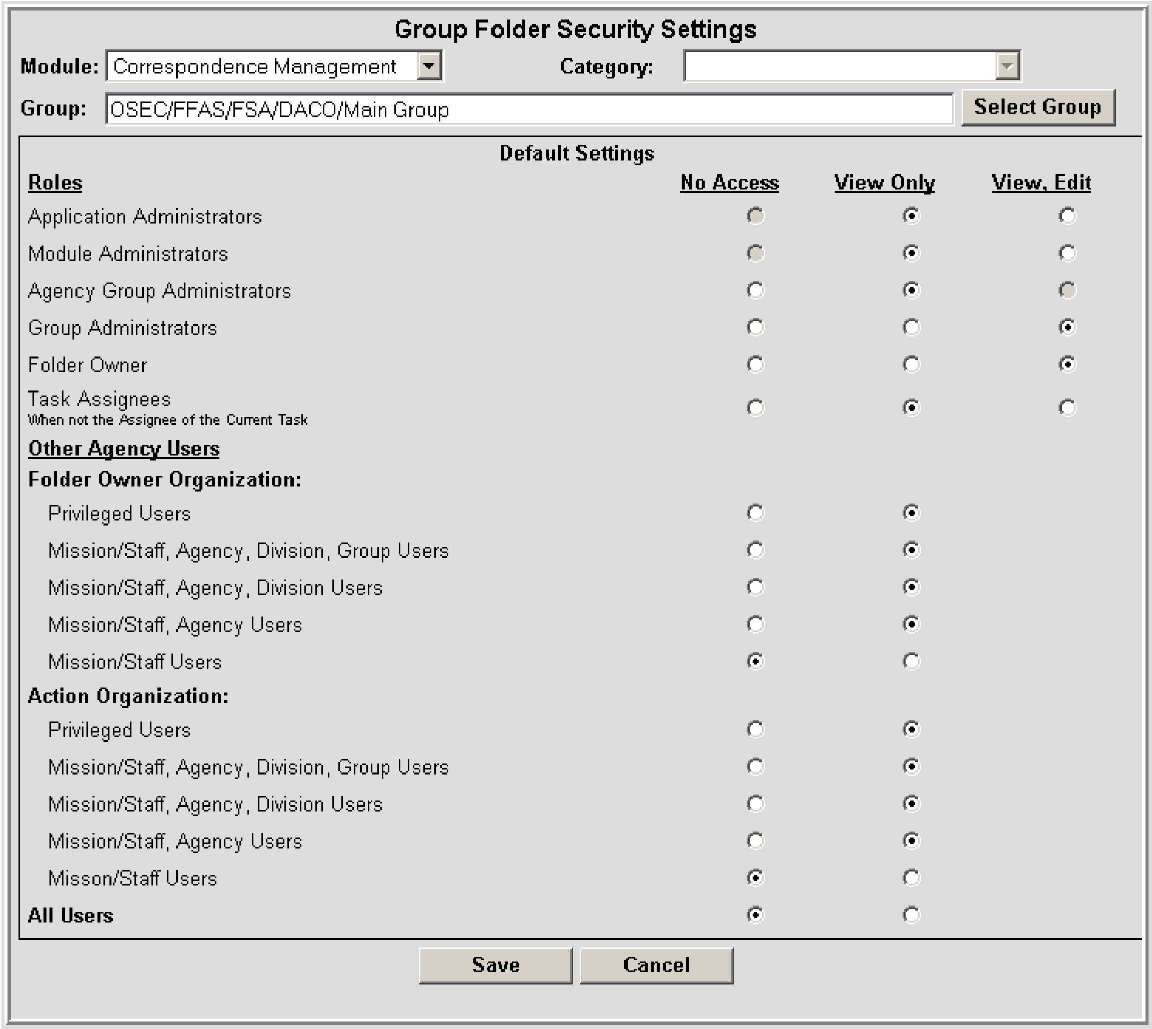


Figure 106: Group Folder Security Settings

Document Security

Document Security automatically defaults to the same settings as Folder Security, but it can be tailored to suit different needs. The Document Security screen in **Figure 32** shows the Operations that can be modified and the security setting options. The security options can be changed for any operation.

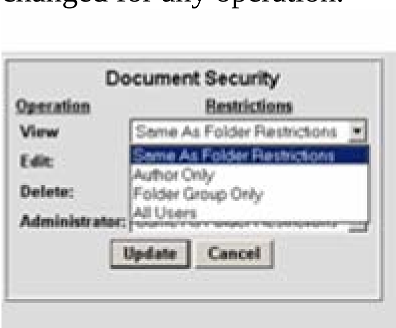


Figure 32: Document Security

Capabilities Based On Organizational Hierarchy

The following diagram shows an example of USDA organizational hierarchy.

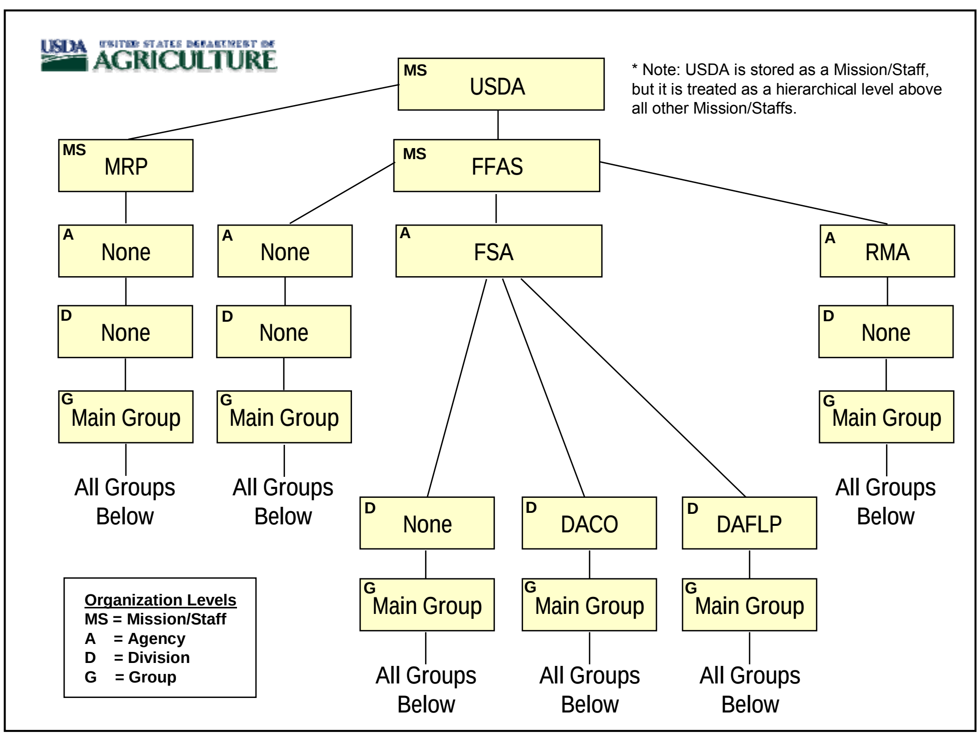


Figure 107: USDA Organization Hierarchy

In ECM, some privileges and defaults are anchored to a specific point in the organizational hierarchy and then apply to all levels (organizations, groups, and users) below. When group default security settings are created, they are anchored to a specific organization and apply to all organizations below unless further restricted by a lower-level group security default. Lower-level security settings cannot be less restrictive than the settings inherited from parent groups.

For example, if a group default security setting is created at the FSA Agency level, it would apply to all folders whose Folder Owner organization is within any group within the FFAS Mission/Staff and FSA Agency.

If the default security setting was created at the DACO level, it would apply to all folders whose Folder Owner is within any group within the FFAS Mission/Staff, FSA Agency, and DACO Division.

This hierarchy also applies to privileged users. The access for a privileged user depends on the organization the privileges are anchored to. The Secretary of the USDA may be a privileged user at the USDA Mission/Staff level. This would grant access privileges to all folders within all organizations in USDA.

If a privileged user is anchored at the DACO Agency level, that user would have access to all folders for all Folder Owning groups within that Division. This user would not be able to access folders in the DAFLP, None, or other divisions within the FSA agency.

Agency Group Administrators are also anchored at an organization level. Agency Group Administrators are automatically set as Group Administrators for all groups within the organization granted and all organizations below. This uses the same hierarchical rules as described above for privileged users and default security settings.

Agency Group Administrators are able to manage all groups within the organization (anchor point and below). They have additional privileges that other Group Administrators do not have:

1. Add/Change Users
2. Add/Change Agency Security Settings
3. Authorize Folder Owning Groups
4. Create Alias-Only Groups

Group Customized List of Values

Group-customized Lists of Values (LOVs) are based on organizational hierarchy.

Managing Privileged User and Agency Group Administrator Designations

A Security Officer may create or remove privileged user and agency group administrator designations as part of the user's profile. The following screens show how to manage these settings for a user.

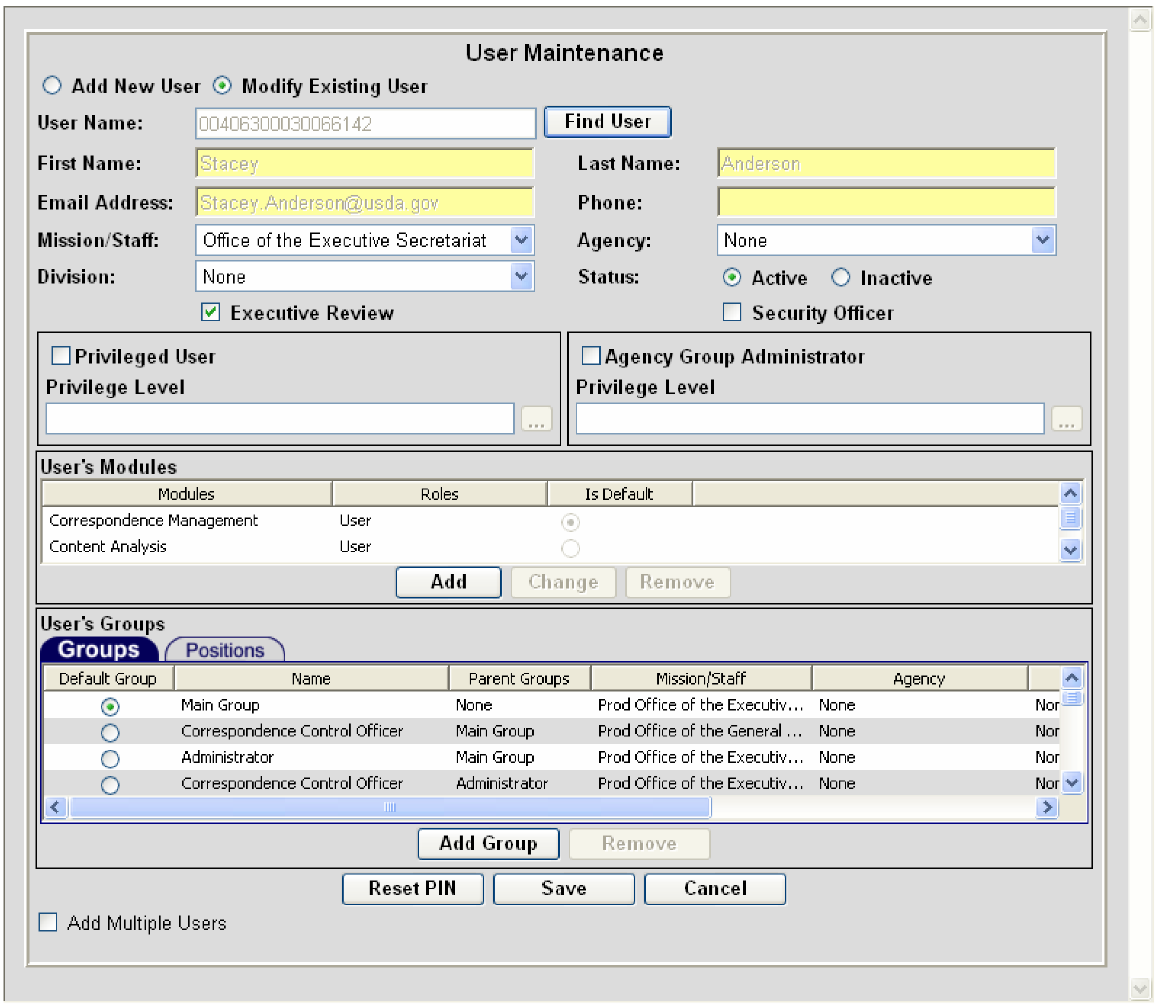


Figure 108: User Maintenance Screen

The User Maintenance screen has two new panels – Privileged User and Agency Group Administrator. Only a security officer may manage these settings.

To set up a Privileged User, the Security Officer clicks the Privileged User checkbox. The Select Privilege Level screen is displayed to define the anchor point within the organization.

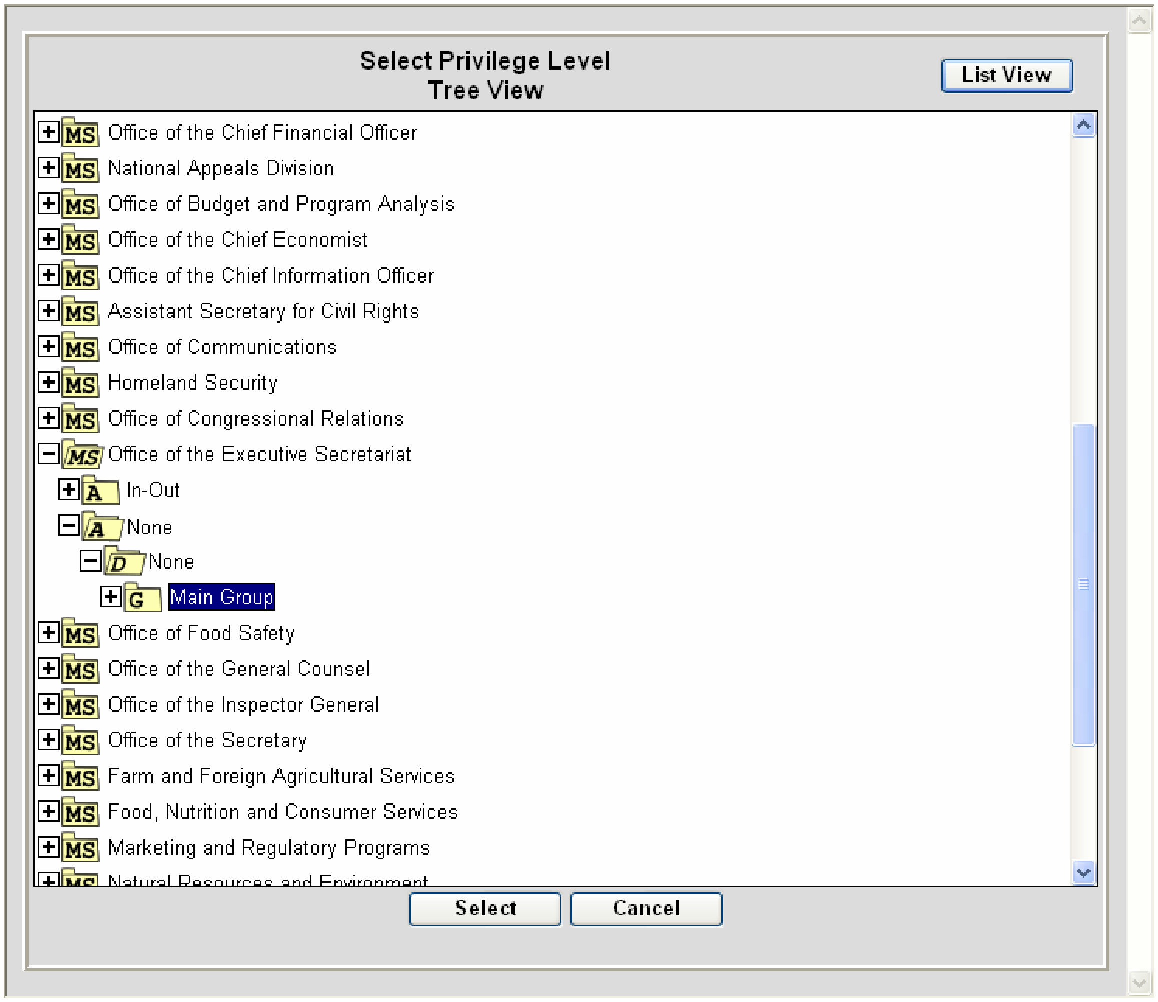


Figure 109: Select Privileged User Anchor Point

With the tree view interface, the Security Officer can navigate to a lower level in the hierarchy by clicking the <+> symbols in the display.

In this example, the security officer selects a group as the anchor point for the privileges. With this selection, the privileges are being anchored at:

Mission/Staff: OES
Agency: None
Division: None
Group: Main Group

The following screen example shows the same selection using the List View interface.

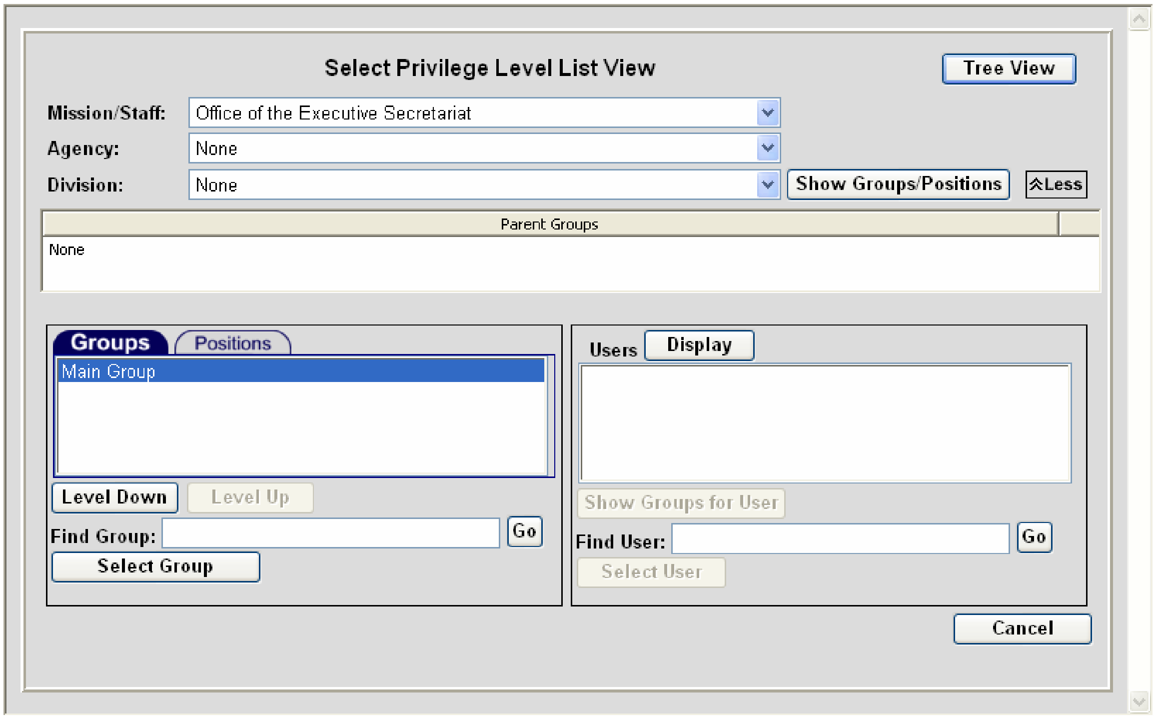


Figure 110: Select Privilege Level - List View

With either interface, the Security Officer clicks the <Select> button, and the privileges are granted. The User Profile is now redisplayed with the updated information.

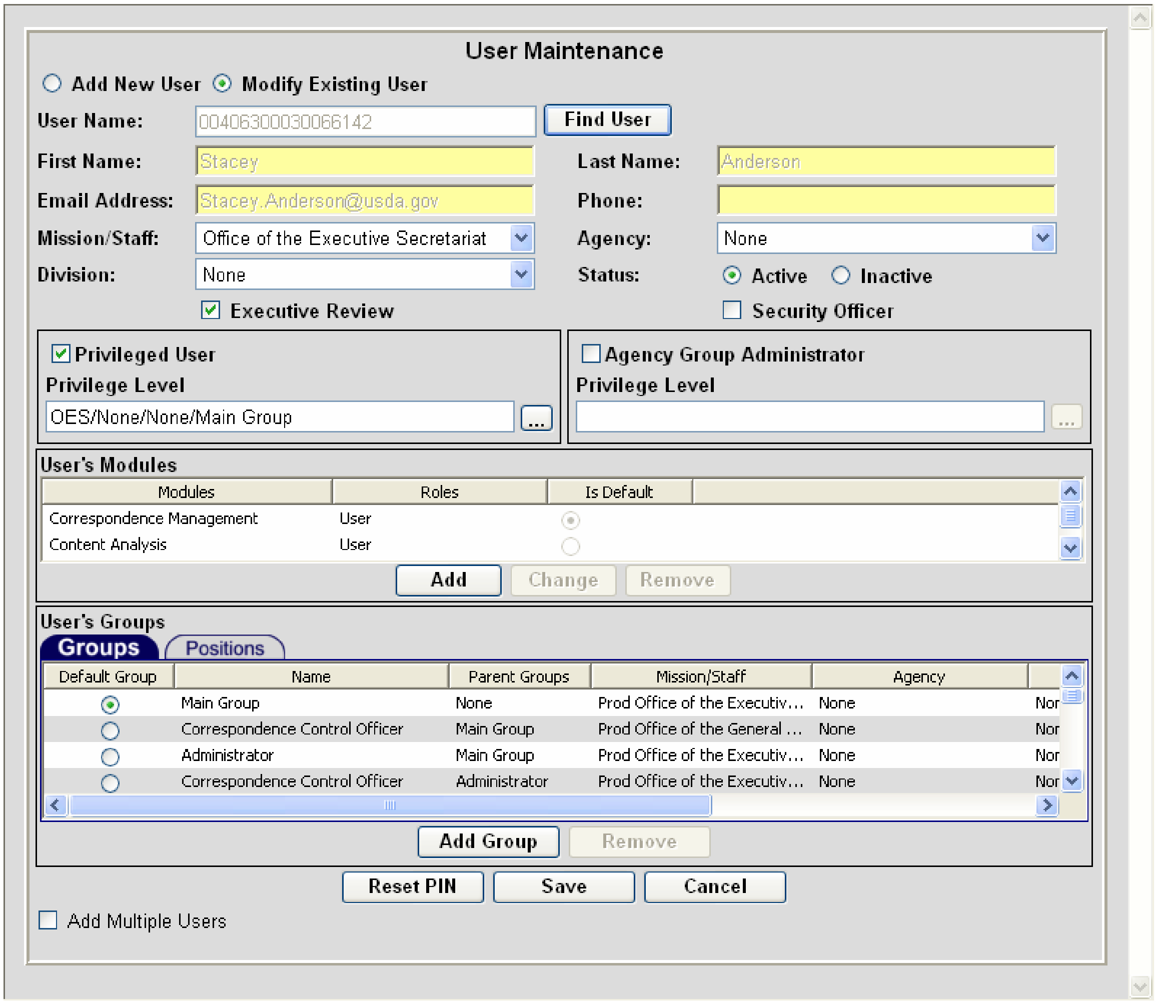


Figure 111: User Maintenance Screen with Privileged User

This user is now privileged and can view all folders whose Folder Owner organization is within the OES/None/None/Main Group level or below.

Now the Security Officer would like to make this user an Agency Group Administrator. The Security Officer clicks the checkbox next to Agency Group Administrator, and the Select Privilege Level screen is displayed.

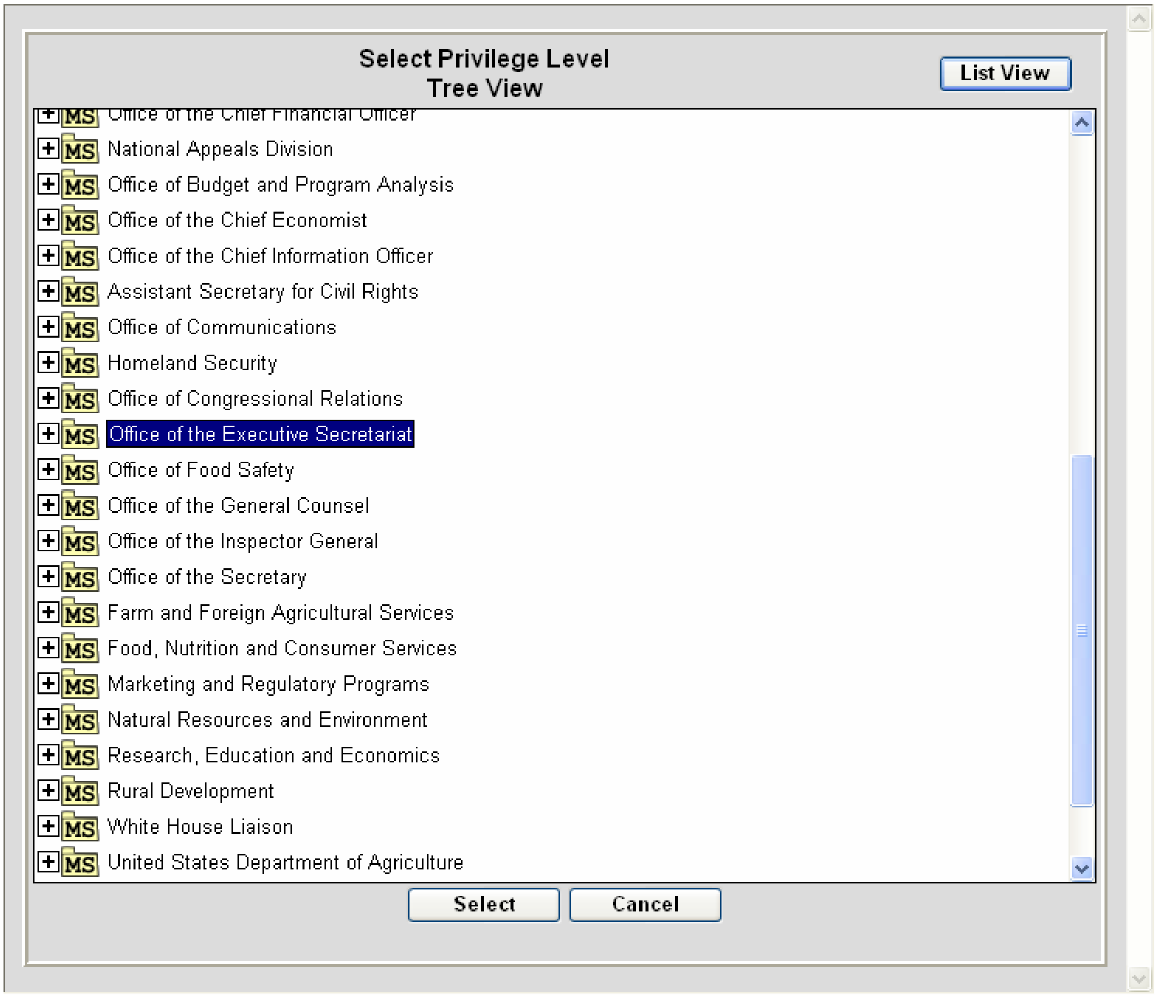


Figure 112: Select Agency Group Administrator Anchor Point

The Security Officer can select any organization at any level in the hierarchy. To select the Mission/Staff of OES and all levels below, the Security Officer highlights Office of the Executive Secretariat and clicks the <Select> button.

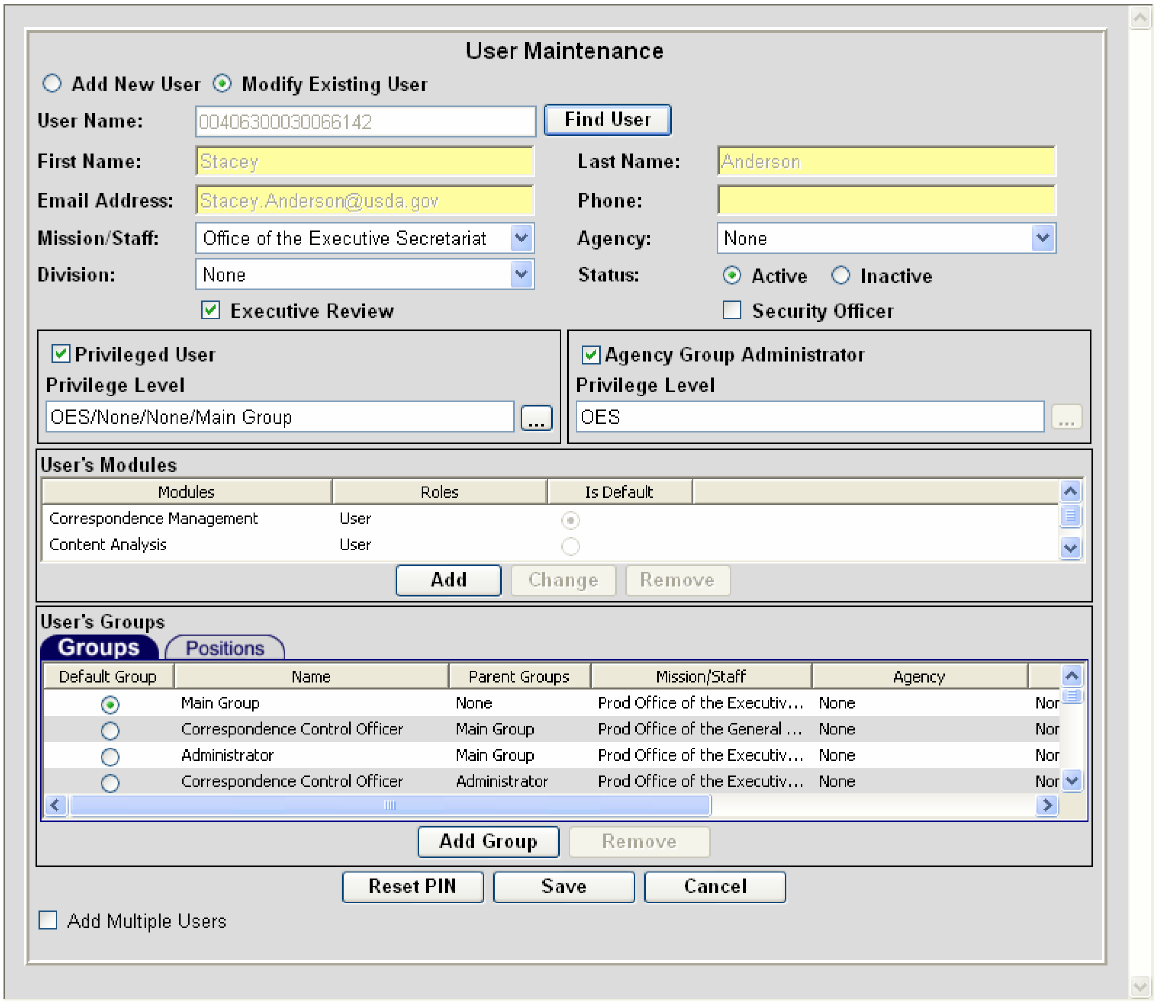


Figure 113: User Maintenance with Agency Group Administrator Privilege

This user is now an Agency Group Administrator for the OES Mission/Staff. This Agency Group Administrator is automatically designated as a Group Administrator for all groups in all agencies and all divisions within the OES Mission/Staff.

The Agency Group Administrator can be anchored at any level within USDA. The privileges apply to all groups within that organizational anchor point and below. When new groups are added below the anchor point, the Agency Group Administrator is automatically added as a Group Administrator for the new group.

The Security Officer can remove the Privileged User designation or the Agency Group Administrator designation by un-checking the checkbox. The user will lose all of the privileges that were granted. If an Agency Group Administrator is made inactive, that user will be removed as an Agency Group Administrator in all of the applicable groups.

ECM Security Officer

The security officer is a specialized class of administrator. The security officer can:

- Add new users (not exclusive; shared with other administrators)
- Make changes to user accounts (not exclusive; shared with other administrators)
- Add/Change Groups (not exclusive; shared with other administrators)
- Designate Privileged Users (exclusive; other administrators cannot designate)
- Designate Application Administrators (exclusive; other administrators cannot designate)
- Designate Module Administrators (exclusive; other administrators cannot designate)
- Designate Agency Group Administrators (exclusive; other administrators cannot designate)

A security officer will only have rights to perform these administrative functions. Security officers will only have rights to view or edit folders within their own organizations and groups. A security officer may not manage his or her own user account.

Only a Security Officer can grant Security Officer privileges to a user. To grant security officer privileges to another user, the Security Officer checks the Security Officer checkbox to grant privileges to the user as shown below.

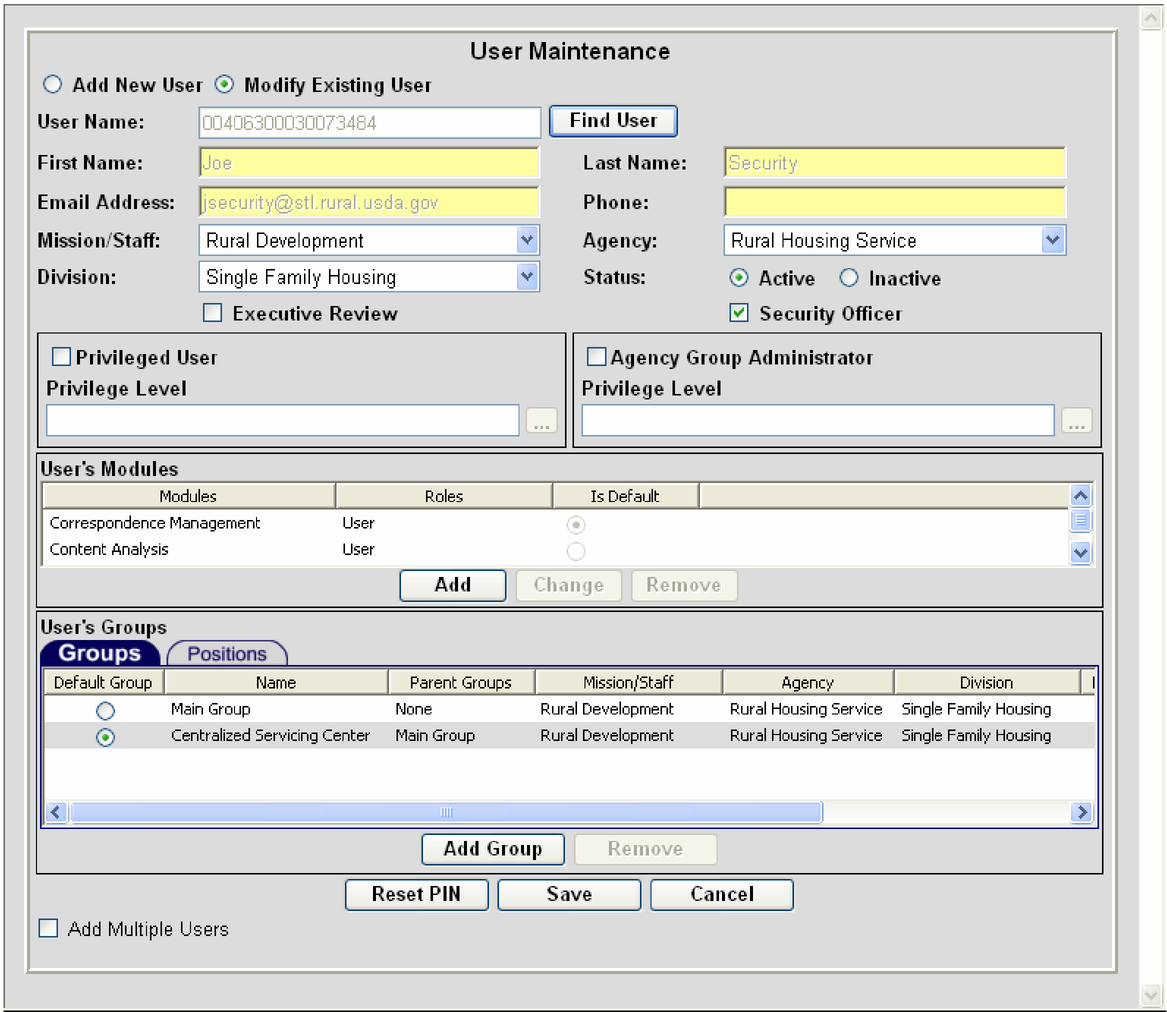


Figure 114: Security Officer Designation

To remove Security Officer privileges, the Application Administrator un-checks the box.

The system creates an audit trail of all accounts added and edited by the security officer. The changes to each account are logged to a database table. Reports can be created so this information can be reviewed on a regular basis.

Authorized Groups

Groups must be authorized in advance before they can be granted the following capabilities:

- Allow to be designated as a Folder Owning Group.
- Add/Maintain Group-Customizable Lists of Values.

To become an authorized folder owning group, the group must have a Group administrator who has attended ECM administration training. Application, Module, or Agency Group

Administrators may designate an authorized group. The following screen example shows the Group/Position Maintenance screen.

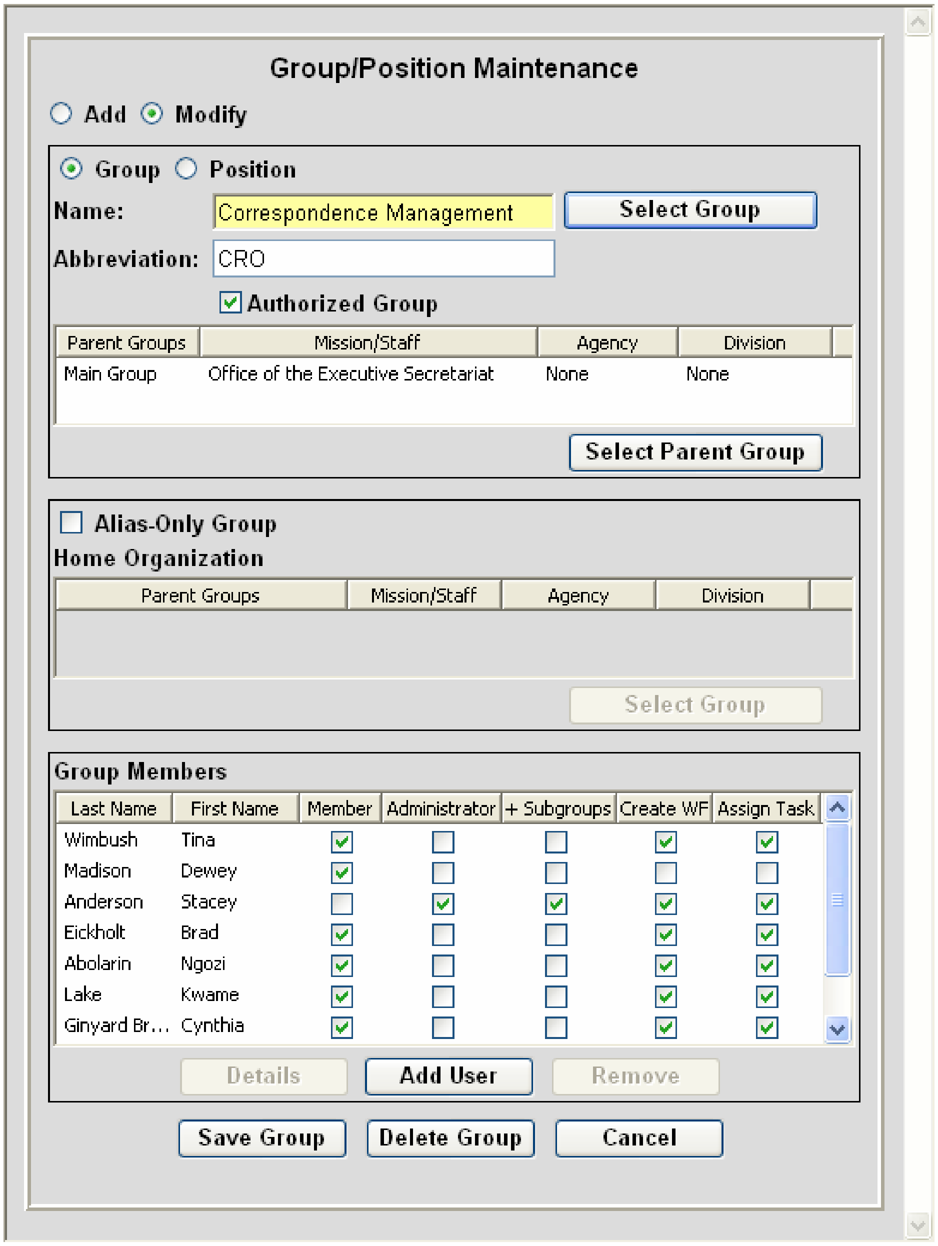
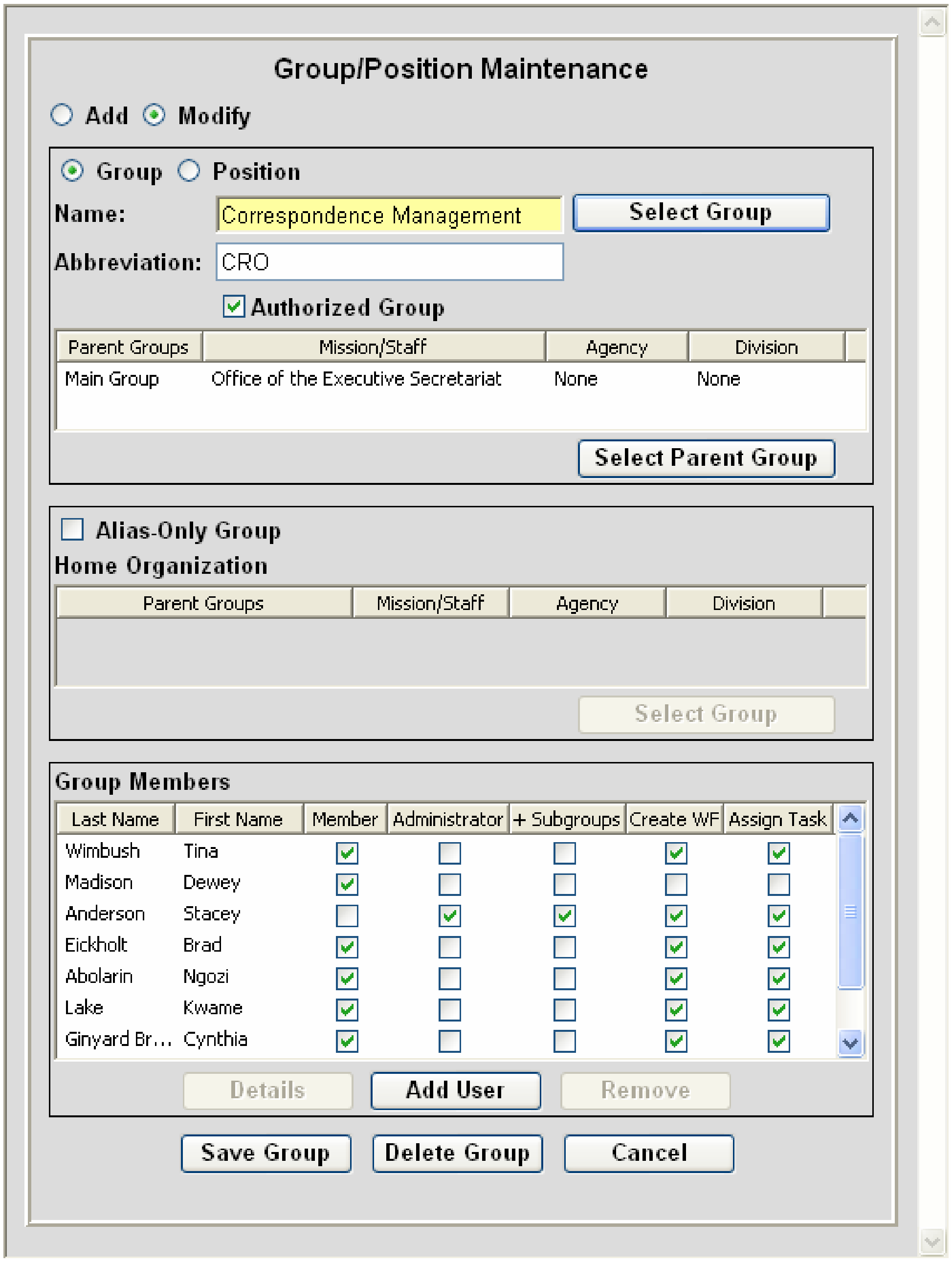


Figure 115: Group/Position Maintenance - Authorized Group

To authorize a group, the administrator checks the Authorized Group checkbox.

Designate Group Administrator for Current Group Only

In ECM, Group Administrators are designated as having Group Administrator for only the designated group. As an additional, and separate, privilege, a Group Administrator can be designated as having Group Administrator rights for subordinate groups (+ subgroup privilege).



When a user is identified as an Administrator for a group, the + Subgroups checkbox designates if the user is also an administrator for subgroups of the designated group. The default is yes (checked), but it may be unchecked. Application, Module, Agency Group Administrators or

Group Administrators for a higher-level group with +Subgroup privilege may designate whether or not the group administrator is an administrator for subgroups.

Alias-Only Groups/Positions

Some groups or positions are created *only* to support the aliasing of workflow tasks. The user(s) in an Alias-Only group belong to a different organization from the one that the Alias-Only group is created within. Alias-Only groups and their users are managed by users with administrative privileges for the owning "home" organization, not the "destination" organization.

An Alias-Only group allows user(s) who perform work for a specific external organization to receive a workflow task when that organization is the action organization for the folder – but the user(s) is not a member of that organization.

Members of Alias-Only groups should not be mistaken as employees of the organization. With access privileges based on the organization, members of Alias-Only groups are excluded from access privileges to organizations they are added to for aliasing purposes. Alias-Only groups also need to be excluded from reports at the agency level

To support these requirements, groups that are created only for aliasing purposes (e.g. CM Agency) will be identified as Alias-Only Groups. They will be excluded from other users in the agency when granting access rights based on the organization.

In Outstanding Tasks reports, Alias-only groups should be excluded from the Action Organization and included for the Folder Owner. The "home" organization for the group is captured so outstanding tasks reports for the home organization will include outstanding tasks for its Alias-Only groups.

The following screen example shows an Alias-Only group.

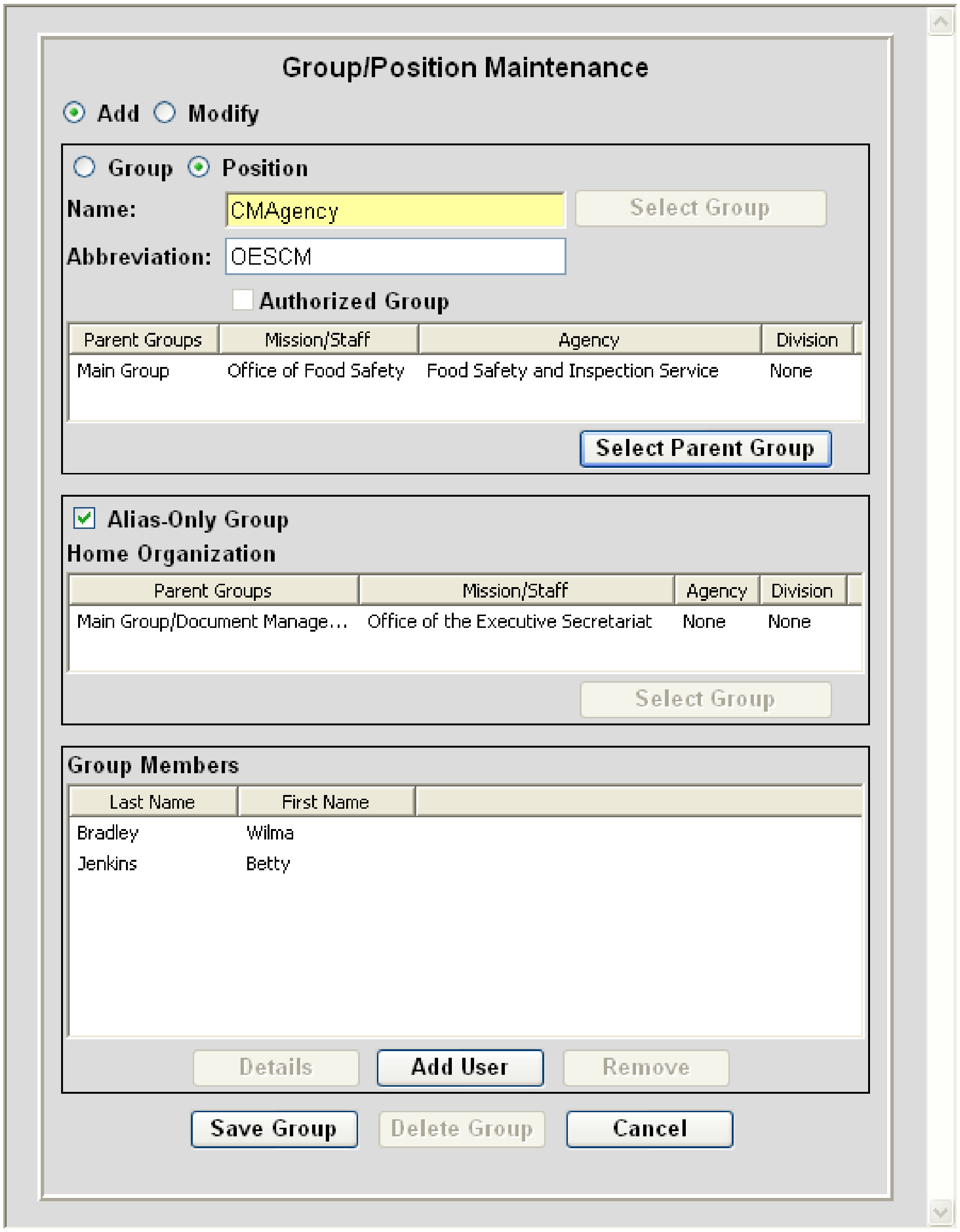


Figure 116: Alias-Only Group / Position

This is actually an Alias-Only Position. The Home Organization is OES/None/None/Main Group/Document Management Group. Only Application, Module or Agency Group Administrators may create Alias-Only Groups or Positions.

Folder Owner Functions

As part of the security re-alignment, the following changes were made to Folder Owner capabilities:

- Folder Owner cannot Close a Folder except when being prompted after completing the Final Task.
- Separate the Close and Re-Open Folder functions. Allow the Folder Owner to Re-Open folders. Only allow an Application, Module, or Group Administrator to Close or Re-Open a folder.
- Remove the capability for a Folder Owner to Complete Tasks or Delete Folders. Only allow an Application, Module, or Group Administrator to perform these functions.

ECM Application Privileges by Role

See the attached spreadsheet that displays which ECM application functions can be performed by various user roles. The user roles are:

Folder Owner
Application Administrator
Module Administrator
Agency Group Administrator
Group Administrator
Task Assignee (for the current task)
Security Officer

The spreadsheet includes Folder functions, Folder Administration, and System, Module and Group Administration.

7. ECM Template Libraries

Currently, ECM supports two types of libraries, one stores document templates and the other stores workflow templates. Document templates are documents, or portions of document, that are stored for repeated use or for reference. Workflow templates are workflows, or portions of a workflow, that are stored for repeated use. Workflow templates can be associated with processing codes, and such templates are automatically inserted into an ECM folder when the associated processing code is added to an ECM folder.

Workflow Templates

Workflow templates are created in the standard workflow editor. Once complete, they can be saved to the Workflow Template Library. Similarly, a Workflow Template can be copied from the library and placed into a folder or into the workflow editor. From the workflow editor, the menu for the workflow list is shown below.

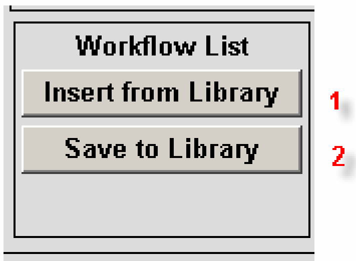


Figure 117: Workflow List Menu

1. Insert from Library

The user is taken to the Select Workflow List shown in the figure below.

The user's default group is shown in the top window. The user may search the lists for another group by clicking the <Select Group> key. The list of workflows for that group is shown in the middle window. When a name on the list is highlighted, the workflow attached to that list is shown in the bottom window.

The user may scroll through the list or may search for a specific workflow by entering a name or a partial name in the 'Search For:' box and clicking <Search>.

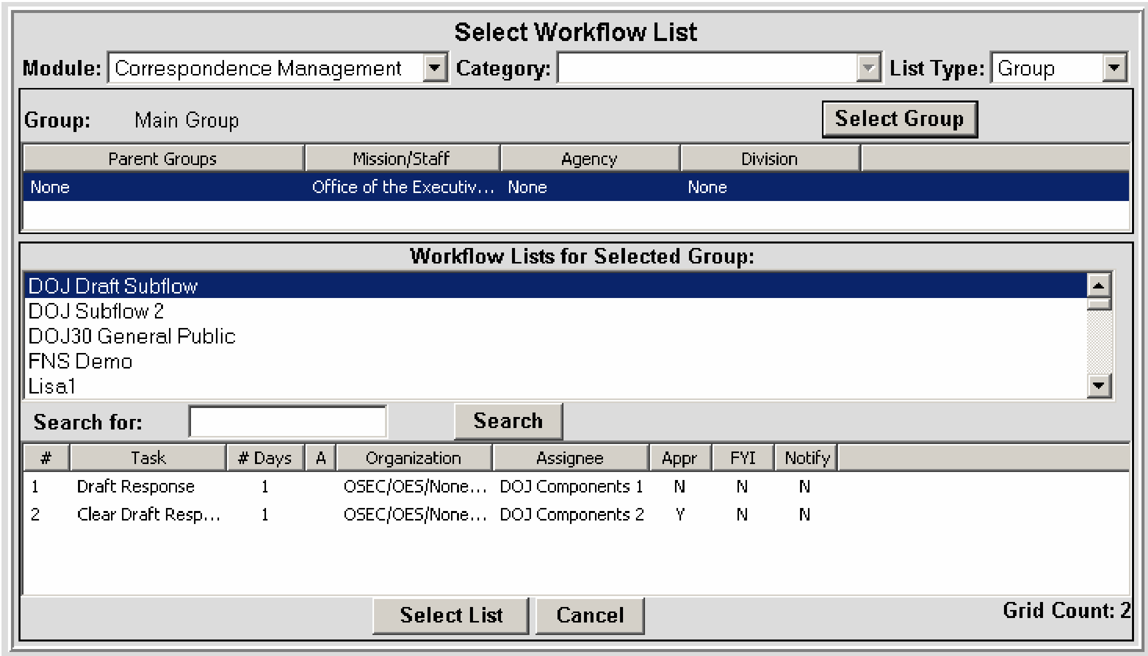


Figure 118: Select Workflow List

The user clicks <Select List> and is returned to the Workflow Editor. If the workflow is complete and needs no changes, the user clicks <Update and Return>. The user returns to the folder with the workflow tab displayed. The new workflow will be shown in the window as seen below. The <Launch Workflow> button is now visible.

2. Save to Library

Once the user has created a workflow that will be used again, it can be saved in the workflow library by clicking <Save to Library>.

If a workflow already exists with that name, a pop-up with an error message will be displayed as seen in the figure below.

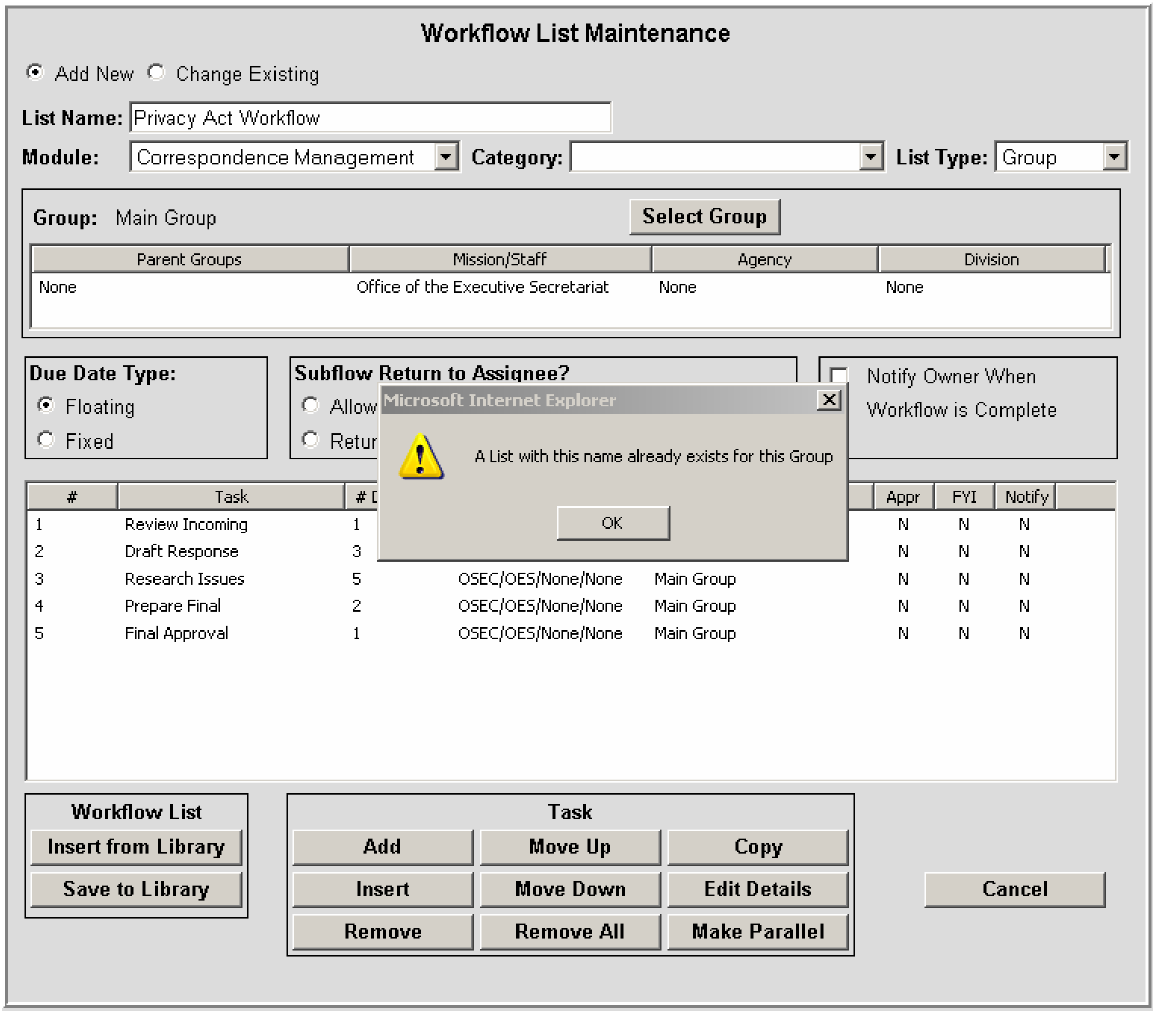


Figure 119: Save Workflow List – Select Existing List Name

Upon clicking <OK>, the user will be returned to the Workflow Maintenance List where the name can be altered as seen below.

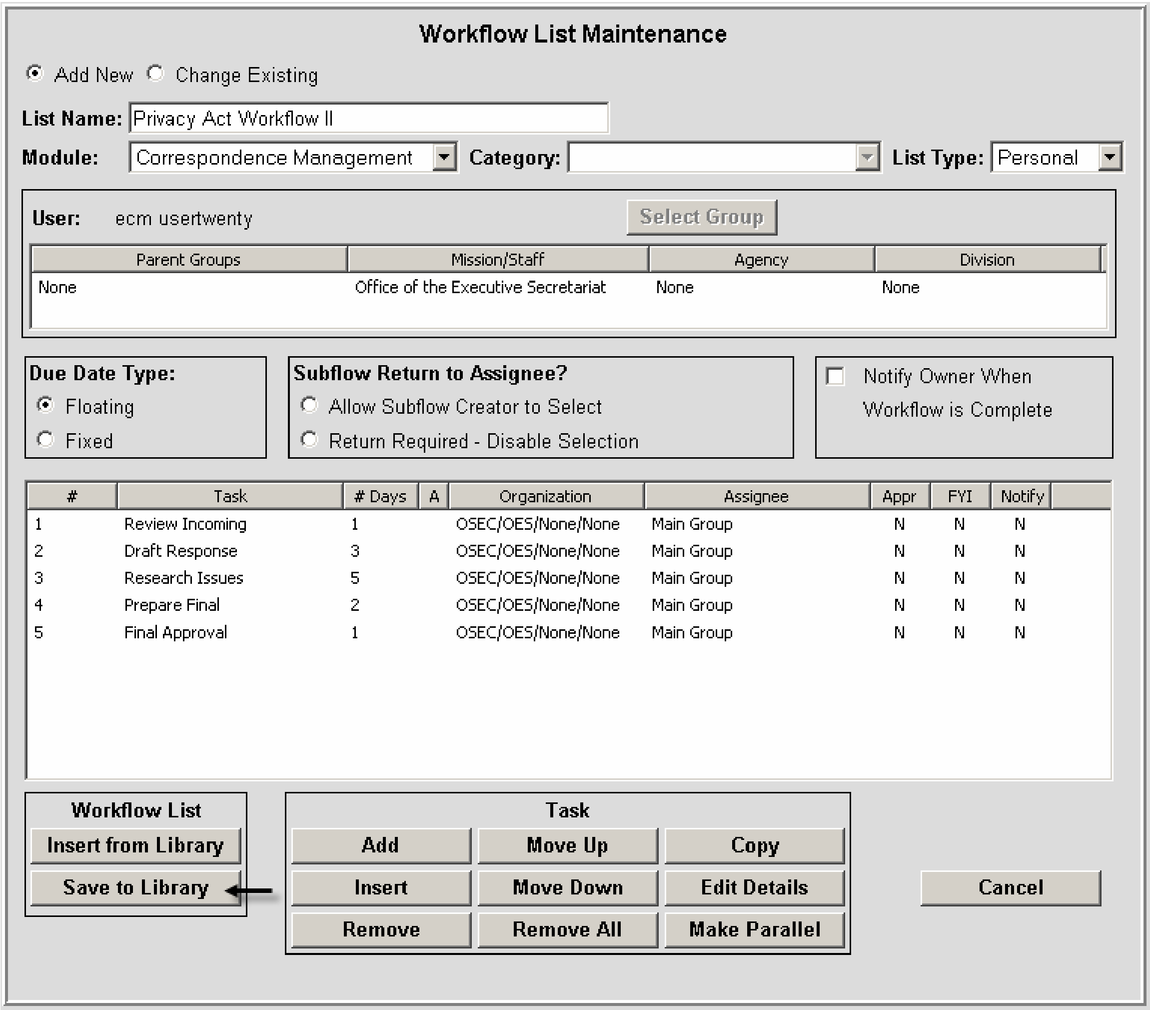


Figure 120: Workflow Maintenance List – List Name Modified

The user can verify that the List has been saved by clicking on <Insert From Library> and searching for the workflow name as seen below.

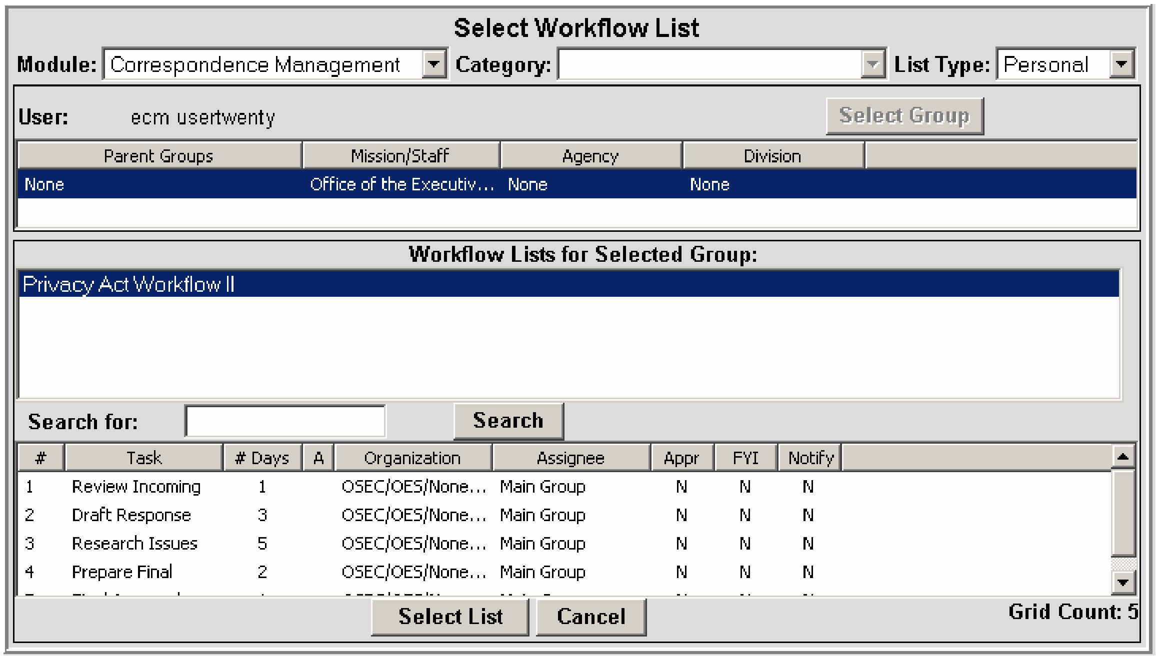


Figure 121: Workflow Maintenance List – List Name

After saving the workflow, the user remains on the Workflow Maintenance List with the worflow intact but without a list name. The user may continue to create or modify personal workflows.

CANCEL

Clicking <Cancel> will return the user to the Main Menu.

Document (Doc) Templates

Document templates are documents, or parts of documents, that are stored in a reference library. The objective of this section is to provide instruction for the addition of document templates for groups within the ECM application. The following screen will be displayed after selecting the *Doc Templates* link on the Administration menu. Templates are associated with a specific group within each module in the ECM application. Templates can be added or modified from this page. Templates should be set up with an expiration date to ensure that no outdated information is kept in the system.

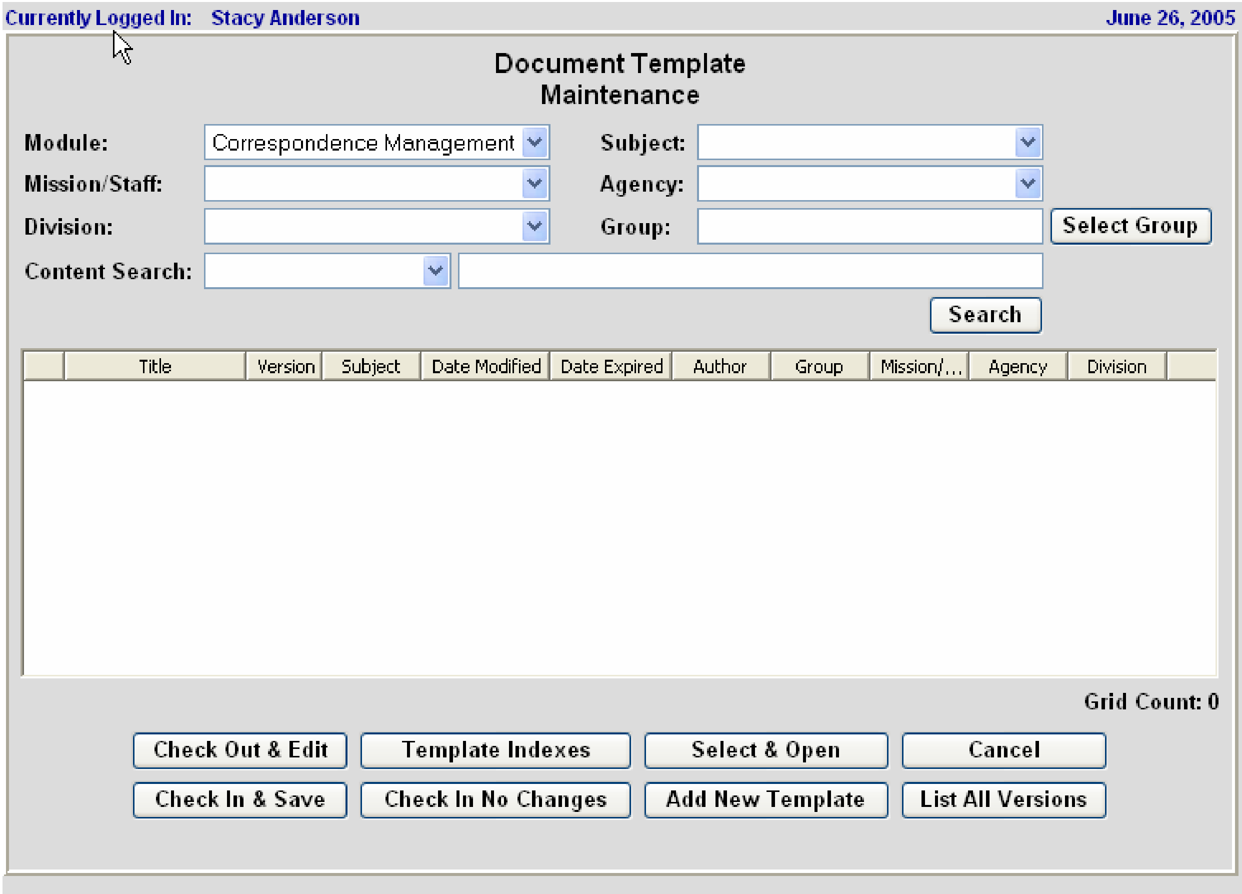


Figure 122: Document Template Library (Document Template Maintenance)

Document Templates

The Document Template button gives the user access to a list of document templates that can be used to create new documents. Initially, the document template screen opens with a list of all templates for the module as seen below.

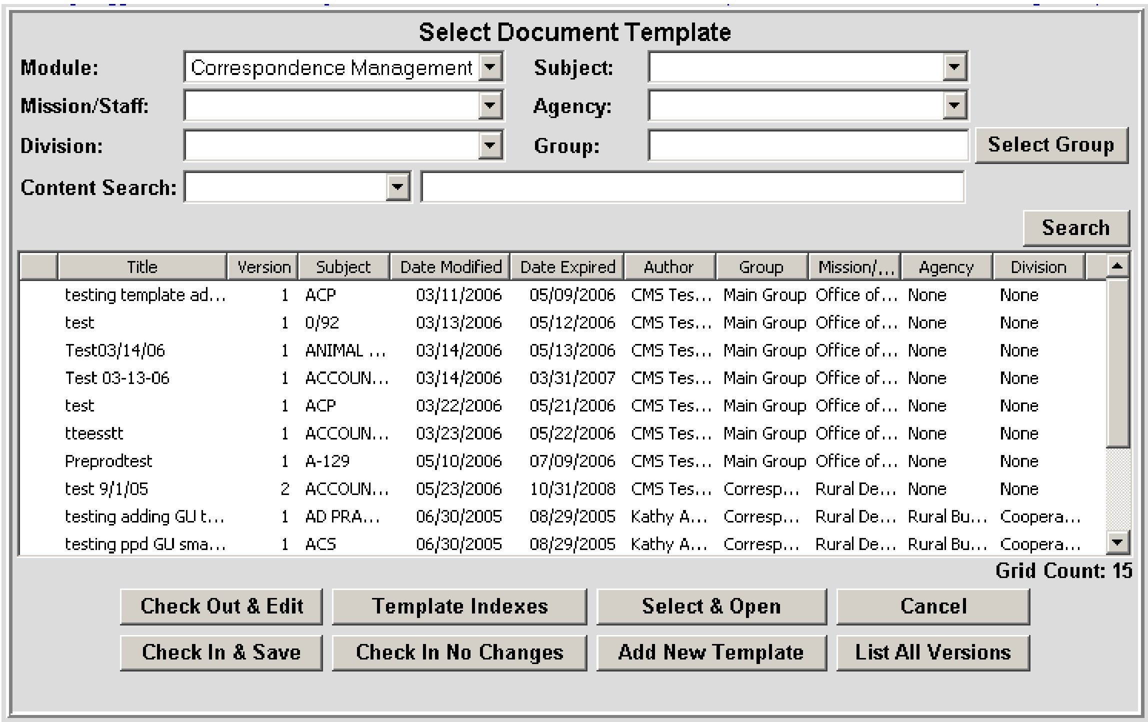


Figure 123: Select Document Template

The user may search for a template by using any combination of Module, Subject, Mission/Staff, Agency, Division, Group or even by content.

ADD NEW TEMPLATE

If a user has a template of a commonly used document and wishes to add it to the template library, this can be done by clicking <Add New Template>. The Window shown in **Figure 34** is displayed.

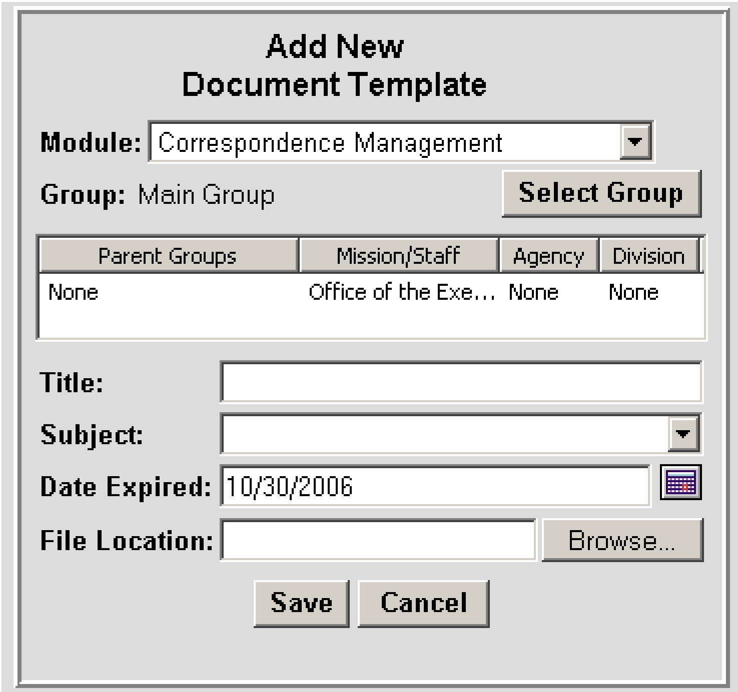


Figure 124: Add New Template

The user may stay in their default user group or choose to save the template in another group by clicking <Select Group>. The user enters the Title and Subject of the template, an expiration date and the file location of the template and clicks <Save>. This will place the template in the Template Library and make it available for other users.

CANCEL

The user may leave the template menu and return to the previous screen.

LIST ALL VERSIONS

Displays the different versions of a changed template. The user may choose the current or a prior version.

CHECK OUT AND EDIT

Checks out the template for editing. The template is locked until checked in.

CHECK IN AND SAVE

Checks the edited template into the library.

CHECK IN NO CHANGES

Changes the status of the template to “checked in” without adding a document to the library.

TEMPLATE INDEXES

Edits the data (such as title) of the document template in the library.

Only users with the appropriate privileges may use these options.