Creating ePM Custom Security Categories

What are Security Categories?

Security Categories contain security roles which gives users access to applications in ePM. When a user is assigned a category, what actions they can perform and what documents they can see is determined by the roles within the category.

The GSA business line has defined several 'baseline' Security Categories. These Categories correspond to project roles (e.g. GSA-PM, EXT-AE Lead, etc.). There are different categories for internal (GSA Staff) and external (EXT Non-staff) users.

There are two sets of Security Roles in each baseline Security Category. The Role Set defines all of the roles, or the *limits* that a user is allowed to have for a given Security Category. The Principal Set contains the *defaults,* or the specific roles a user will inherit when they are exported to a project with that Category.

Who Will Use This?

√ ePM System Administrators

√ ePM Trainer (Administrator)

Why should ePM Trainers or ePM System Administrators have access to create custom Security Categories for their regional programs?

Although ePM allows it, the GSA security auditing rules forbid adding or deleting roles from individual user accounts at the Project level. All Security Categories are defined and managed at the Program Level. In other words, the roles any user has on any project *must match exactly* the Principal Set of roles of the nominal category they possess.

When a user requires roles that are not included in the Principal Set of one of the baseline Security Categories, a Custom Category may be created, provided the following conditions are met:

- The Custom Category is based on one of the approved baseline categories
- The name of the Custom Category follows the naming convention (described below)
- The Principal Set of the Custom Category does not exceed the limits of the Role Set of the baseline Category on which it is based.

It is considered a serious breach of security for a user to possess any security roles that are not included in the Role Set of the Baseline Category.

The ePM system will permit a System Administrator or ePM Trainer to create a cloned custom Category for their program or specific project needs. There is an expectation that, if audited, no user will possess more or fewer security roles than the Principal set of the nominal Security Category they possess.

Creating Custom Categories

The GSA will periodically audit Security Categories using the 'Administration and Audit Utility' (See QRG.109 Administration Audit Utility). Because this utility parses the Category name in order to determine the set of security roles to validate against, Categories must follow a very strict naming convention. Below is an example of the Base Category Configuration Naming convention in addition to a Custom Category Naming convention.

DEFAULT Category Base Category Name

EXT-CMa (Read Own)	• Where '**EXT'** represents External Users and CMa represents their project Roles, such as Construction Manager as an Agent

Custom Category Base Category Name

CC EXT-CMa (Read Own)	• **Name must begain with 'CC'** • CC must be followed by the exact/**base category name** on which the cc is based. CC's must be derived from a current versio baseline category. • **(Description of custom category)** should describe how/why it is different tha the default category and contained within parenthesis.

The following are steps to create and setup a custom security category:

1. Log into ePM as a user with the ePM Trainer or ePM System Administrator security role and enter Program workspace.

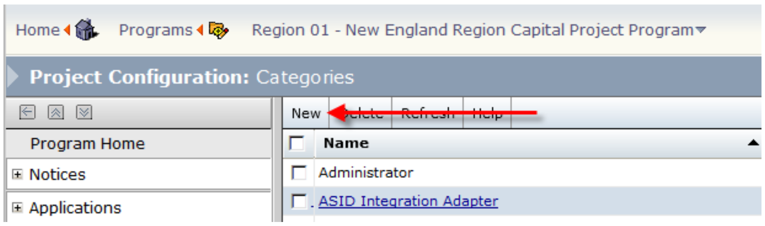
2. Select the Program of preference to create a custom category.

3. Navigate to Administration > Project Config. (Managed) > Security > Categories.

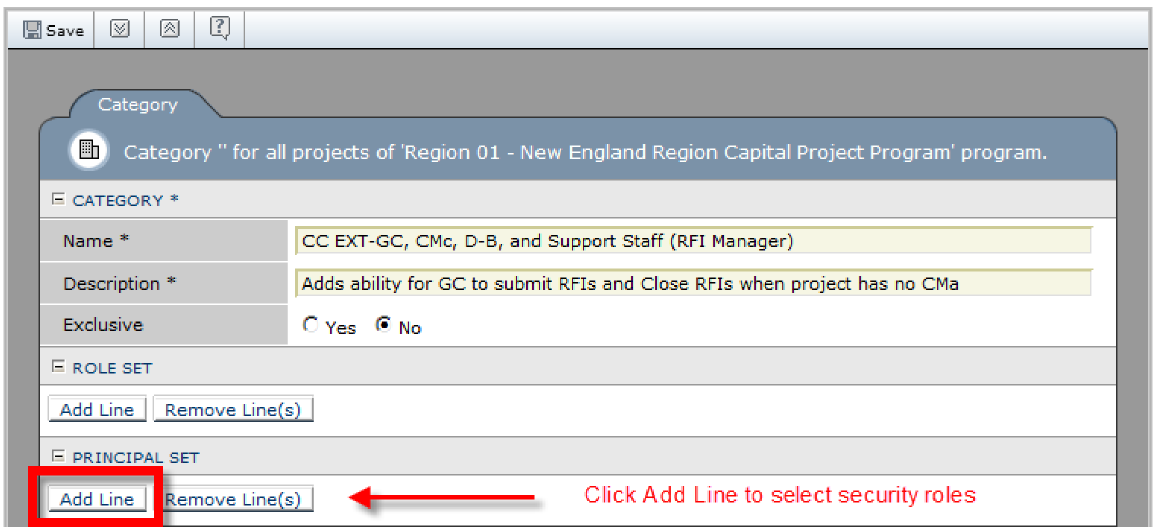
4. Click on the "Base Category" of preference to launch the category document desired to clone as a custom category (EXT-Read Only, EXT: AE-Lead, etc.)

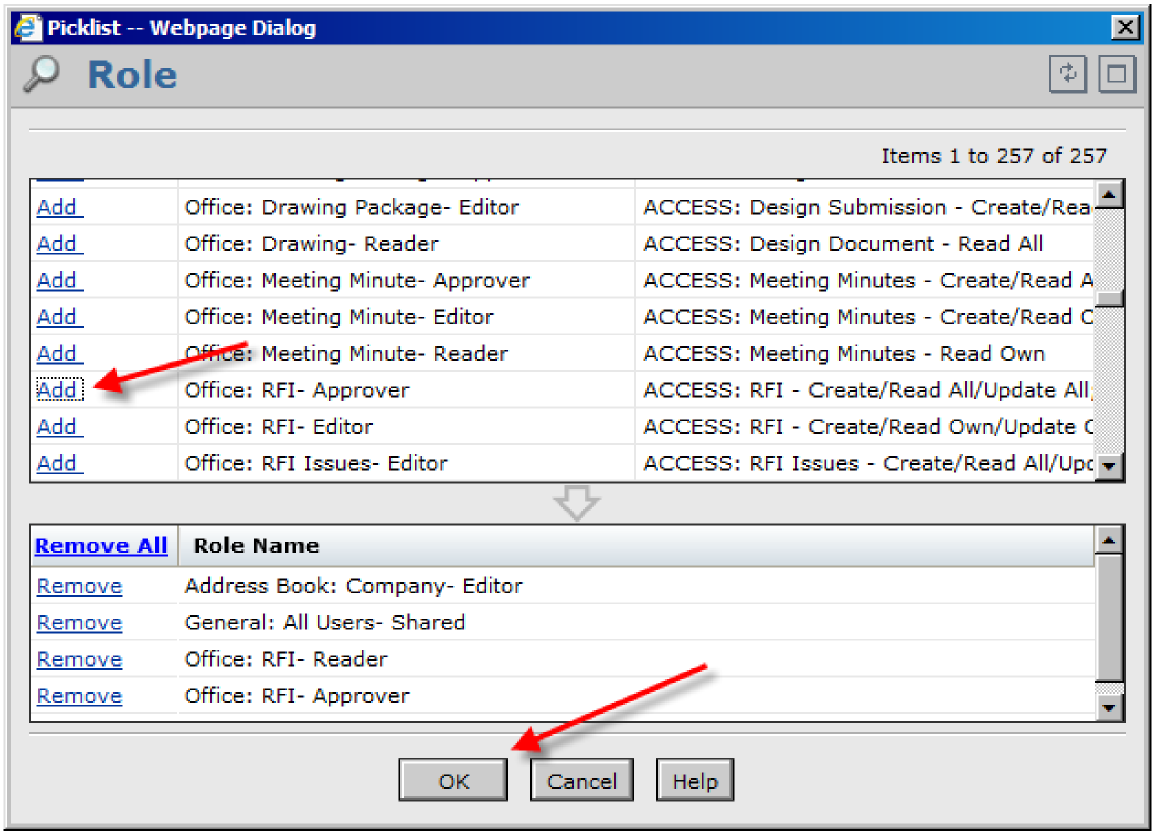
5. Take a screenshot of all ‘Principle Set’ roles assigned to the base security category and Close the Category document by selecting the “X” in the upper-right corner of the document.

6. Click on ‘New’ from the Category register toolbar to create a new custom category.

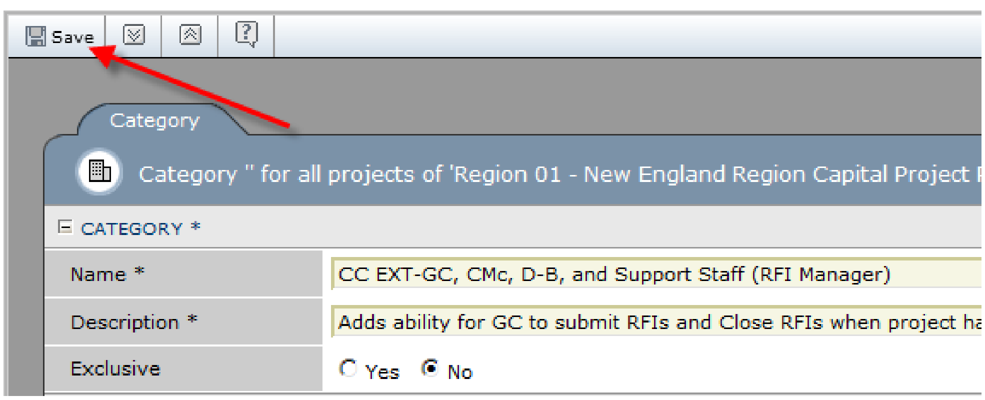


7. Click on ‘Add Line’ from the ‘Principle Set’ section to add multiple roles that reflect the screenshot of all base security roles to be cloned for the custom category.





8. Click Save and close the document.

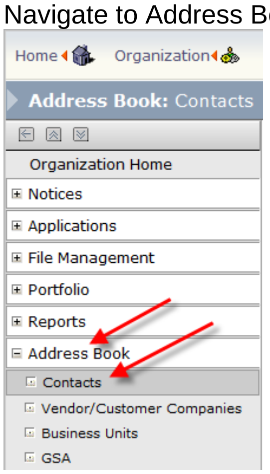


Re-Exporting Contacts to Inherit New Security

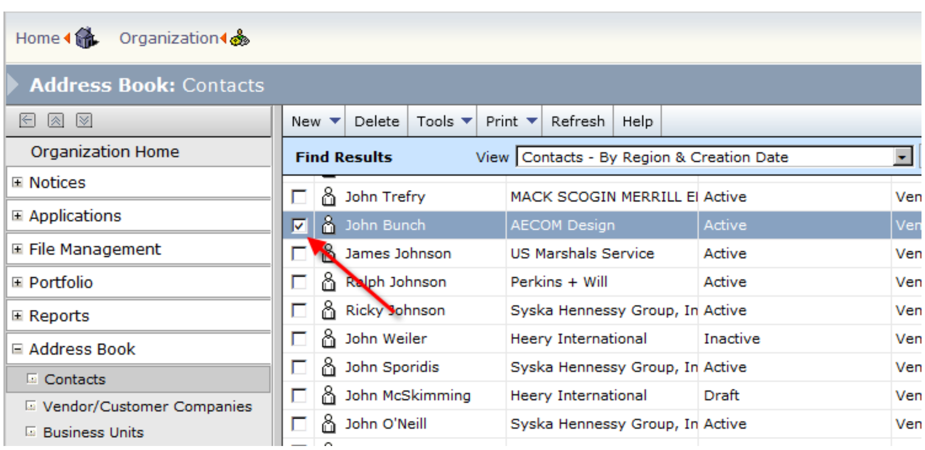
Once the above steps have been completed, it is important that the contact is re-exported to the project overwriting the previous security role for that user on that project.

1. Enter the Organization Workspace.

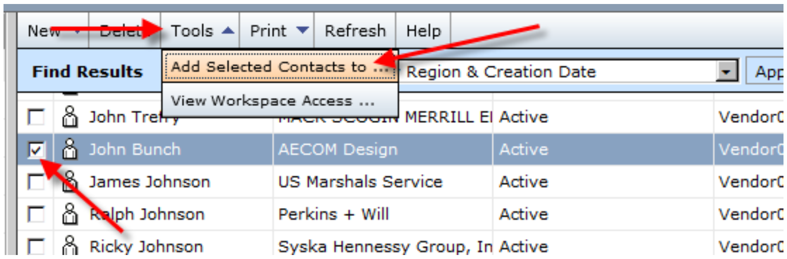
2. Navigate to Address Book > Contacts or Staff. The Address Book Register displays.



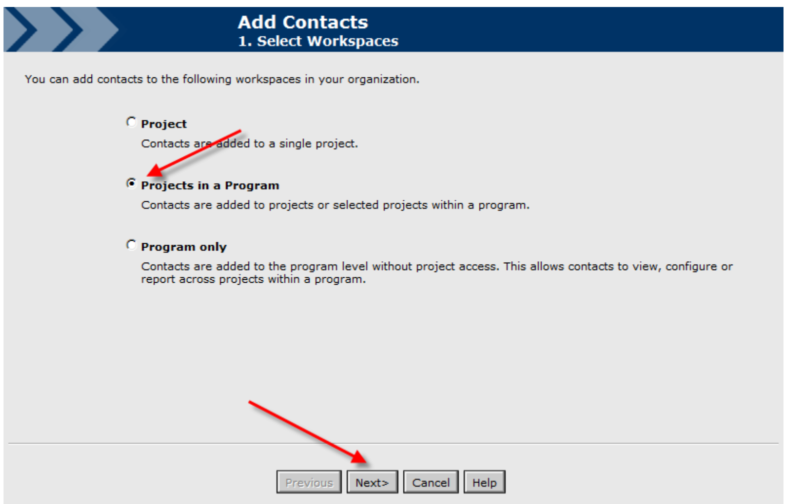
3. Locate the Contact(s) for whom the Custom Security Category were created, place a checkmark in the box to select.



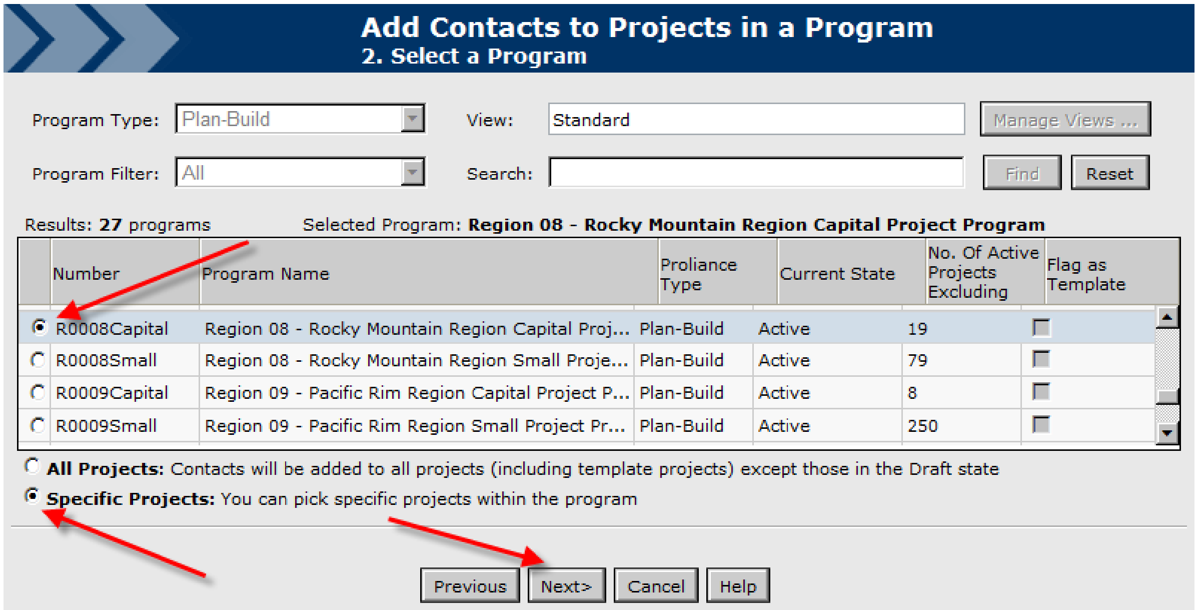
4. In the Menu bar, select Tools > Add Selected Contact to … or Staff to … (this will vary depending if the goal is to export staff or contacts)



5. Select Projects in a Program > click Next**.**

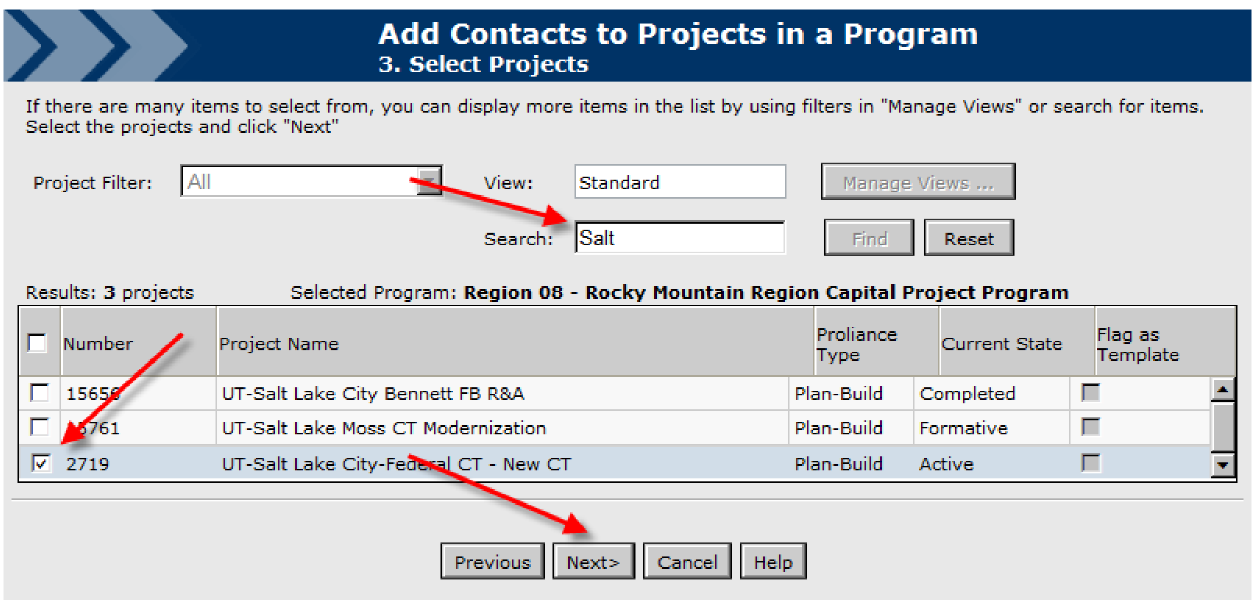


6. Select Program where the contact(s) or staff will be added to by clicking radio button >valiate that "Specific Projects" is selected below > click Next.

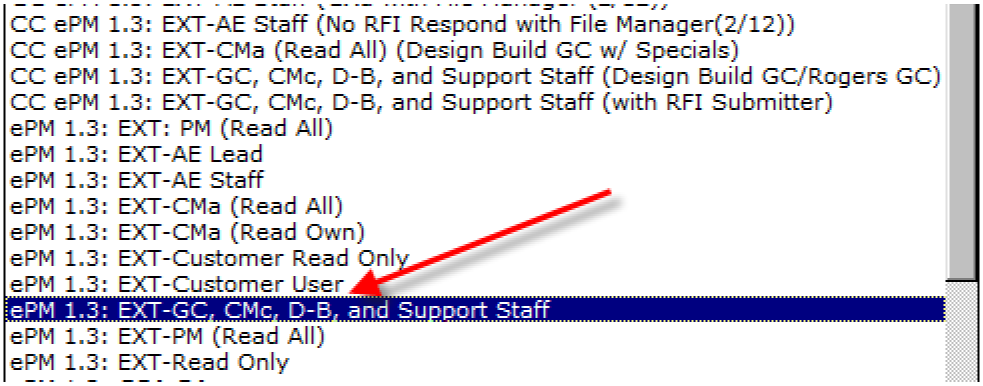


7. Select Project(s) where the contact(s) or staff will be added to by placing a checkmark in the box > click Next.

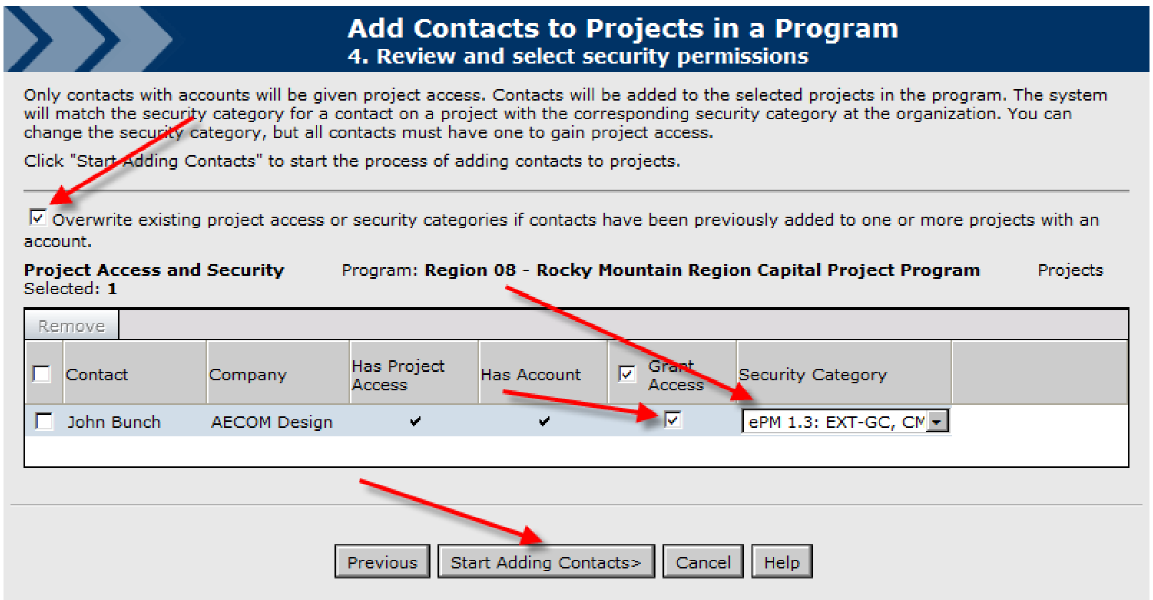
Hint: Use the Search box to narrow the project list down to a more manageable size.



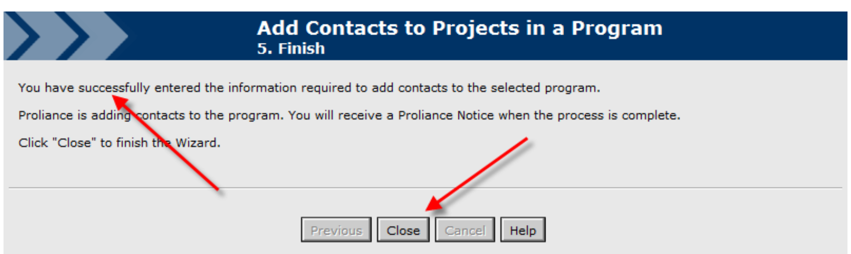
8. Select the appropriate Security Category from the drop down list for each contact.



9. Check the box next to “Overwrite existing project access or security categories if contacts have been previously added to one or more projects with an account.” > click Start Adding Contacts.



10. Validate that the final window confirms that the Security Category was applied successfully, then click Close.



Tips

- √ It is imperative that we do not extend the visibility of ACR – Cost specific data to the external user base unless they are assuming a CMa responsibility. If the GSA PM would like to allow a GC or other non external user access to access ACR (budget) data or give them all instance access, they will need to get this authorized.

- √ **IMPORTANT:** ePM System Administrators and ePM Trainers in each region must manage these custom security categories especially as ePM evolves through iterations of deployment versions and hot fixes. If Meridian Systems ever changes the configuration to the base categories (usually for integration or Office Business Applications (OBA) purposes), it is critical for the ePM System Administrators and ePM Trainers to obtain and understand the delta of such configuration to determine if those same changes need to be applied to their custom categories; therefore, avoiding failures and high support call volumes.